ANÁLISIS DE RIESGOS Y DIAGNÓSTICO DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ESE HOSPITAL SANTA MÓNICA, BAJO LOS PARÁMETROS DE LA SEGURIDAD INFORMÁTICA.

JONATHAN ARISMENDI RAMÍREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DOSQUEBRADAS
2017

ANÁLISIS DE RIESGOS Y DIAGNÓSTICO DELA SEGURIDAD DE LA INFORMACIÓN DE LA ESE HOSPITAL SANTA MÓNICA, BAJO LOS PARÁMETROS DE LA SEGURIDAD INFORMÁTICA.

JONATHAN ARISMENDI RAMÍREZ

Proyecto de Grado para optar al título de Especialista en Seguridad Informática

Asesor: Ing. JULIO ALBERTO VARGAS
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DOSQUEBRADAS
2017

Nota de aceptación:

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Pereira, Diciembre de 2017

DEDICATORIA

Este trabajo de Grado se lo dedico a Dios, por darme la salud y fortaleza, para emprender nuevos retos, y no desfallecer en el camino.

A mis padres quienes con su ejemplo y tenacidad, han sido las personas que me mostraron el camino correcto, y me enseñaron que para lograr grandes cosas, requiere de dedicación y de creer en uno mismo.

A mi esposa Tania Largo y a mi hijo Santiago Arismendi, quienes han sacrificado su tiempo y espacio; y han sido los motores que me impulsaron en las dificultades en aras de llevar este proyecto personal a feliz término.

AGRADECIMIENTOS

Agradezco a la ESE Hospital Santa Mónica, en cabeza del Dr. Javier Alejandro Gaviria, quien en conjunto con la Coordinadora del Área de Sistemas de Información Sandra Echeverry, avalaron la realización del presente proyecto al interior de la Institución.

A mi familia en general por el sacrificio que realizaron en tiempo y espacio, para que yo pudiera llevar a feliz término, este nuevo reto en el proceso de aprendizaje continuo, que me enriquece a nivel personal y profesional.

Al Esp. Ing. Julio Vargas, quien con su tiempo, dedicación y metodología; logro encaminar en poco tiempo el presente proyecto, para culminarlo de la manera adecuada.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

En la actualidad todas las organizaciones comparten un elemento en común y el cual es su activo principal; la información y los datos. En ella se encuentra, todas las evidencias del actuar administrativo y misional de cada empresa, por lo que para realizar toda su gestión (captura, procesamiento, y entrega de resultado), se debe acudir a la implementación de sistemas de información, que adicionalmente garantice su custodia, almacenamiento y recuperación.

Para la implementación de un sistema de información; sin importar la magnitud del mismo; se debe recurrir al uso de equipos de cómputo, redes de datos locales; que incluye además transmisiones de datos e internet, para la comunicación entre los diferentes canales. Por lo tanto, las redes de datos, además de permitir y agilizar el manejo de la información al interior de la empresa, puede convertirse en una puerta de vulnerabilidades, dejando en riesgo cada uno de los elementos que hacen parte del sistema de información y en especial los datos.

Por lo anterior, una de las prioridades para la Gerencia de Tecnología de la Información, debe ser el garantizar el cumplimiento de los elementos fundamentales que establece la Seguridad de la Información, como lo son la Disponibilidad, Integridad y Confidencialidad. La reducción de este riesgo, puede alcanzarse aplicando de forma permanente y estandarizada, mejores prácticas desde la infraestructura interna de la entidad, hacia el exterior; ya que estas pueden ser de cualquier tipo y pueden originarse desde diferentes fuentes.

Teniendo en cuenta esta situación, toda empresa debe estar preparada para reducir o eliminar cualquier tipo de riesgos de éste tipo. En caso de que se materialice, la empresa debe contar con herramientas para disminuir su impacto y la afectación en los servicios misionales, gerenciales y administrativos.

Con el desarrollo del presente proyecto se pretende identificar debilidades, vulnerabilidades y riesgos presentes en la infraestructura de redes de datos de la E.S.E Hospital Santa Mónica.

1. PLANTEAMIENTO DEL PROBLEMA

La E.S.E. Hospital Santa Mónica, es una institución que presta servicios de salud, de primer y segundo nivel de complejidad, en el municipio de Dosquebradas departamento de Risaralda. Con la necesidad de ampliar su portafolio de servicios, y debido a la gran demanda que se genera desde el régimen subsidiado y vinculado hacia la empresa; ésta se ha visto obligada a realizar; de forma muy apresurada y sin ningún tipo de planeación; la ampliación de su plataforma tecnológica, que los ha obligado a realizar cambios e implementaciones; de forma improvisada y sin ningún tipo de proyección previa.

En este proceso de crecimiento corporativo, se han involucrado una serie de aliados estratégicos, que no poseen conocimientos sobre el escenario tecnológico de dicha entidad; y adicionalmente no cuentan con una infraestructura de redes de datos propia; por consiguiente con ningún otro elemento tecnológico acorde a dicha infraestructura. Este aspecto ha desencadenado desorganización y poco control sobre las redes y los datos, todo esto sumado a la ausencia de políticas de Tecnologías de Información en la institución.

Otra situación que impacta directamente al sector salud del país, y particularmente a la E.S.E Hospital Santa Mónica, es el gran volumen de normatividad vigente y su alta frecuencia de cambios, la cual exige diversas y complejas implementaciones, la automatización de procesos tales como Historia Clínica, intercambio de datos entre entidades, automatización de los procesos contractuales del estado, control de insumos y servicios y su facturación; el control de cartera con los diferentes actores del sistema nacional de seguridad social en salud, el presupuesto institucional, entre otros.

Todos estos procesos no son solo complejos, sino vitales para la estabilidad de esta entidad, los cuales se podrían ver altamente impactados; si adicionalmente no se cuenta con los controles suficientes y adecuados para la protección en el acceso a servidores, bases de datos, así como datos clínicos, administrativos y financieros; lo que deja en un alto riesgo la estabilidad de la Red de datos Corporativa y la confidencialidad de información catalogada por diferentes normas, como altamente sensible.

La E.S.E Hospital Santa Mónica, no cuenta con políticas de seguridad de la información, claras que respondan por la disponibilidad, integridad y confidencialidad de la información y solo se realizan incipientes procesos de organización y adopción de normas.

Otro componente importante es el recurso humano, que en una mínima proporción corresponde a personal fijo; ya que por ser ésta una entidad del

sector público; aproximadamente el 95% de sus colabores, está contratado a través de empresas temporales que proveen el recurso humano. Esto origina una alta rotación de personal misional y de apoyo; el cual deja sin control de estos a la entidad; un aspecto que bajo la óptica de la seguridad informática atenta contra uno de sus pilares fundamentales.

Por lo anterior, se genera la necesidad de realizar una identificación de debilidades, vulnerabilidades y riesgos, enfocada a la infraestructura de redes de datos, con el fin de dar las recomendaciones, para su posterior mitigación por parte del área encargada en la institución.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo minimizar las amenazas y vulnerabilidades presentes en la infraestructura de redes de datos que afectan la seguridad de la información de la E.S.E. Hospital Santa Mónica?

2. JUSTIFICACIÓN

La ESE Hospital Santa Mónica, es una institución del sector público, que presta servicios de salud en el Municipio de Dosquebradas Risaralda, a través de modalidades de evento y contratación por cápita, para lo cual suscribe convenios y/o contratos, con diferentes Entidades responsables de pago.

Los resultados de dicha atención, son registrados a través de un software asistencial, el cual almacena la historia clínica de los pacientes atendidos en la institución. Dicho software es integral y totalmente en línea con los demás módulos asistenciales y administrativos, y conecta en tiempo real la Sede Principal y los Centros de Atención Ambulatoria, permitiendo y logrando un repositorio de información que consolida la información institucional, con un histórico de quince años.

Las diferentes bases de datos de la entidad, son un activo intangible; ya que contiene datos de altísimo valor; debido a que está conformada por todos los movimientos financieros, administrativos y contables. Dichas bases de datos también; almacenan todo el registro; de acuerdo a la Resolución 1995 de 1999 y Resolución 839 de 2017; de atenciones, registros y conductas médicas que desde lo asistencial, se realizan a los más de 59.000 clientes con que cuenta la entidad y que son los pacientes de los regímenes subsidiado, contributivo y regímenes especiales. Esta información está catalogada como de reserva legal y sensible para su propietario

Es de vital importancia velar por su integridad y custodia; ya que bajo el amparo de la Constitución Política, es un documento de carácter confidencial, sobre el cual solo tiene derecho de acceso el dueño de la historia clínica, el personal médico asistencial tratante y los organismos judiciales. Tampoco se puede dejar de lado, los resultados de todo el accionar de la entidad, los cuales son medidos a través de indicadores, gerenciales, administrativos y de producción, que buscan avalar la viabilidad de la entidad, y que permite el flujo de recursos, para su funcionamiento.

Además de los informes a los diferentes entes de control y vigilancia, que se constituyen en un factor determinante, para el desarrollo del presente proyecto, ya que estos están regulados por un sinnúmero de normas; que no solo exigen el contar con Historia Clínica automatizada, sino que se debe garantizar la integralidad de la misma; así como también dispone los parámetros técnico legales, para el reporte de información a los diferentes organismos.

Por lo tanto, se hace necesario que se planeen estrategias tendientes a garantizar la seguridad de los datos como lo exige la ley en materia de historia

clínica, presupuesto, cartera, estados financieros, los lineamientos de la Estrategia de Gobierno en Línea y la Ley de Protección de Datos.

El presente proyecto pretende auditar la seguridad de la información, a esta importante Institución de salud de la región, optimizando y aprovechando nuevas tecnologías de la información y la comunicación, incrementando su competitividad empresarial; a partir de la identificación de las vulnerabilidades y la posterior entrega de las recomendaciones; que siendo implementadas por la institución, pueden llegar a mitigar los riesgos que se encuentran presentes en la infraestructura de la red de datos, y así propender el cumplimiento de los principios de Integridad, Confiabilidad y Confidencialidad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis e identificación de riesgos, a la infraestructura de redes de datos de la E.S.E. Hospital Santa Mónica de Dosquebradas Risaralda, que sirva como insumo para el aseguramiento de la red de datos de la entidad y seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar cada uno de los componentes de tipo Hardware que hacen parte de la infraestructura de la red de datos de la Institución.

- Ejecutar un *hacking* ético, apoyado en las herramientas disponibles de *Pentesting*, basadas en software libre, con el fin de identificar las vulnerabilidades y riesgos a los que se encuentra expuesta la infraestructura de la de redes de datos de la entidad.

- Generar las recomendaciones de acuerdo a los hallazgos detectados sobre la infraestructura de la red de datos, para su posterior mitigación por parte de la entidad, de acuerdo a los resultados obtenidos en las fases previas y al *hacking* ético.

- Diseñar un plan de mejora, de acuerdo al diagnóstico arrojado que impacte directamente cada una de los hallazgos encontrados a la infraestructura de la red de datos de la Entidad.

- Entregar informe técnico al responsable del área de sistemas de información, que contenga: Los hallazgos, El plan de mejoramiento y las acciones a implementar. Todo lo anterior enfocado a la toma de conciencia por parte de la institución, en beneficio de la preservación de la seguridad de la información.

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES

Con la visión de dar al proyecto de grado, un enfoque acertado, se tomó como referencia los siguientes proyectos en el área de seguridad informática; los cuales reposan en el repositorio de proyectos de grado de la Universidad Nacional Abierta a Distancia (UNAD); y de esta manera aprovechar las similitudes presentadas en las diferente empresas objeto de estudio; con el fin de orientar el desarrollo del presente trabajo.

- Inicialmente se consulta la tesis de grado presentada en Mayo de 2015 en la Universidad Nacional Abierta a Distancia (UNAD), titulado: Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo, Santander, desarrollado por Cordero Moreno José Leonardo y García Reyes Yadimyr Oswaldo, como requisito para optar al título Especialista en Seguridad informática.[1]

La tesis de grado presentada realiza un análisis y evaluación de riesgos bajo la metodología Magerit utilizando la herramienta EAR PILAR, con el fin de entregar una serie de recomendaciones a la institución objeto de estudio para que implemente los controles necesarios, y de esta manera poder minimizar las vulnerabilidades encontradas, en beneficio de la seguridad de la información institucional.

La revisión de este trabajo permite identificar la similitud existente con la propuesta actual, ya que se desarrolla sobre una Institución de Salud de carácter público, y brinda algunas bases para encontrar la manera de abordar la identificación de riesgos y los métodos utilizados, que pueden aportar en el proceso de detectar las afectaciones que se presentan directamente sobre la red de datos de la Institución objeto de estudio en el presente trabajo.

- Siguiendo con la revisión de trabajos relacionados con la ejecución del presente trabajo, se consultó el Proyecto de Grado presentado en el año 2017, en la Universidad Nacional Abierta a Distancia (UNAD), titulado: Proponer un sistema de diagnóstico y monitoreo que permita identificar eventos para resolver problemas de infraestructura de TI, de la red de datos de la Empresa Sociedad Clínica Emcosalud, desarrollado por Celis Perdomo Cesar Augusto y Trujillo

[1] CORDERO MORENO, José Leonardo y GARCÍA REYES Yadimyr Oswaldo Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo, Santander [On line], [consultado el 23 de octubre de 2017]. Disponible en Internet: repository.unad.edu.co/handle/10596/6366

Murcia Francy Patricia, como requisito para optar al título Especialista en Seguridad informática.[2]

Esta revisión, permite identificar nuevas herramientas, aplicables al análisis de la Infraestructura de la red de datos, donde juega un papel importante la observación directa de los componentes y su entorno. La importancia que tienen las entrevistas realizadas a los funcionarios encargados del área de Sistemas de información, quienes ya cuentan con la identificación de algunos aspectos relevantes y críticos, que pueden afectar directamente la red de datos. Finalmente la evaluación de algunas herramientas de monitoreo de redes, que permiten identificar otro tipo de riesgos que pueden llegar a no ser tan visibles.

4.2 MARCO CONCEPTUAL

En la actualidad, donde la mayor parte de las organizaciones han centrado atención en la Información Electrónica; se ha visto obligado a invertir grandes sumas de dinero y esfuerzos en la implementación de diversos aplicativos para la captura, procesamiento, y almacenamiento de datos; buscando el rápido acceso y la eficiencia en su procesamiento.

Sin embargo no se puede olvidar que, todo esto ha sido posible gracias, a que existe un físico para dicha transmisión y son las Redes de Datos; las cuales a través de sus diferentes componentes como (Centros de Datos, *Switches*, *Routers*, Cableado, etc); permiten la comunicación y transferencia de los datos, a través de redes locales de diferente naturaleza.

Sin embargo en la actualidad, ha ido en aumento la cantidad de ataques cibernéticos, a través del aprovechamiento de las vulnerabilidades, presentes en la infraestructura tecnológica y más específicamente en las redes de datos no aseguradas adecuadamente.

Por lo tanto se deben identificar cuáles son los riesgos asociados, con el fin de dar las recomendaciones adecuadas que sirva como base, para la mitigación de los mismos por parte de la Institución objeto de estudio.

4.2.1 Seguridad de la información. Se puede definir como el cumplimiento de las confidencialidad, integridad y disponibilidad de la información y de los datos

[2] CELIS PERDOMO, Cesar Augusto y TRUJILLO MURCIA, Francy Patricia. Proponer un sistema de diagnóstico y monitoreo que permita identificar eventos para resolver problemas de infraestructura de TI, de la red de datos de la Empresa Sociedad Clínica Emcosalud. Bogotá: Universidad Nacional Abierta y a Distancia, 2017

que se tienen de la organización, sin importar el formato que tengan (electrónicos, papel, Audios, videos, entre otros). [3]

4.2.2 Seguridad Informática. GÓMEZ, Álvaro presenta la siguiente definición: "Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema".[4]

4.2.3 Principios de la Seguridad Informática: Los principios fundamentales de la Seguridad informática son la Confidencialidad, Integridad y Disponibilidad. BUSTA, María José los define de la siguiente manera:

4.2.3.1 "Confidencialidad: Esto significa que la información sólo está siendo vista y utilizada por las personas que están autorizadas a acceder a ella.

4.2.3.2 Integridad: Esto significa que cualquier cambio a la información por parte de un usuario no autorizado es imposible (o al menos detectado), y los cambios por los usuarios autorizados son registrados y rastreados.

4.2.3.3 Disponibilidad: Esto significa que la información es accesible cuando los usuarios autorizados lo necesiten".[5]

4.2.4 Seguridad de redes informáticas. Es la propiedad con que cuentan las redes de permitir solo el acceso a dispositivos y personal autorizado, blindándolo

[3] ISOTools Excellence. "ISO 27001: ¿Qué significa la Seguridad de la Información?". {En línea}. {consultado el 05 de Noviembre de 2017} disponible en:(http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion).

[4] GÓMEZ, Álvaro. "Enciclopedia de la Seguridad Informática. 2ª edición". {En línea}. { consultado el 17 de Febrero de 2018} disponible en: (https://books.google.es/books?hl=es&lr=&id=Bq8-DwAAQBAJ&oi=fnd&pg=PT2&dq=define+seguridad+informatica&ots=dwlbZj3gaJ&sig=bIOP5Y7p4Cvd6-ZavJfXfm4rFkw#v=onepage&q=define%20seguridad%20informatica&f=false).

[5] BUSTA, María José. "Principios Básicos de Seguridad TI". {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (https://www.hostname.cl/blog/principios-basicos-de-seguridad-ti)

contra los demás accesos indiscriminados, mediante el uso de técnicas, metodologías y dispositivos a nivel físico o lógico.

4.2.5 Riesgo Informático. Es la condición a la que se encuentra expuesto un sistema informático que puede afectarlo, en cualquier momento en su integridad o en cualquiera de sus componentes; estos se pueden presentar por la incorrecta aplicación de configuraciones, por vulnerabilidades detectadas a nivel de hardware, software, o por amenazas lanzadas indiscriminadamente.

4.2.6 Auditoría. Es la metodología utilizada para verificar las políticas, procesos y procedimientos implementados al interior de la empresa; por medio de esta se busca identificar el funcionamiento adecuado de las directrices implantadas; y en caso de hallar incongruencias o el mal funcionamiento de las mismas, genera una serie de observaciones y recomendaciones para que se tomen las medidas correctivas y se implementen los respectivos planes de mejoramiento que conlleven a la normalización de los elementos antes descritos como deben ser.

4.2.7 Políticas de Seguridad. Son el conjunto de directrices implementadas en las organizaciones con el fin de encaminar el funcionamiento de cada uno de los procesos del sistema de información de una manera adecuada, que permitan garantizar la integridad, confidencialidad y disponibilidad de la información.

4.2.8 Red de Datos. PÉREZ, Julián y MERINO María la definen de la siguiente manera:

> "Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos."[6]

4.2.9 Tipos de Redes: VIALFA, Carlos presenta la siguiente definición:

> "Se distinguen diferentes tipos de redes (privadas) según su tamaño (en cuanto a la cantidad de equipos), su velocidad de transferencia de datos y su alcance. Las redes privadas pertenecen a una misma organización. Generalmente se dice que existen tres categorías de

[6]PÉREZ, Julián y MERINO María. "Definición de Red de Datos". {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (https://definicion.de/red-de-datos/).

redes: red de área local (LAN), red de área metropolitana (MAN) y red de área extensa (WAN).

4.2.9.1 Redes LAN. LAN significa red de área local. Es un conjunto de equipos interconectados entre sí generalmente pertenecen a la misma organización, y, además, están conectados dentro de un área geográfica pequeña mediante algún tipo de cableado de red, por medio de conexión inalámbrica o por ambos medios.
La característica principal de este tipo de redes es compartir recursos o servicios entre los diferentes equipos interconectados (Archivos, impresoras, almacenamiento, internet, entre otros).
La versión más simple de una red es una red de área local. La transferencia de información en una red de área local puede alcanzar hasta 100 Mbps de velocidad (por ejemplo, en una red tipo *Ethernet*) y 1 Gbps (por ejemplo, en redes FDDI o Gigabit *Ethernet*). Una red de área local puede soportar 100, o incluso 1.000, usuarios.

Al extender la definición de una red LAN con los servicios que ofrece, se pueden definir dos modos operativos diferentes: de igual a igual y cliente/servidor. En una red "de igual a igual", la comunicación se realiza de un equipo a otro, sin un equipo central y en el que cada equipo tiene la misma función, mientras que en un entorno "cliente/servidor", un equipo central brinda servicios de red para los usuarios.

4.2.9.2 Redes MAN: Una MAN (red de área metropolitana) interconecta diversas LAN cercanas geográficamente (en un área de unos cincuenta kilómetros) a alta velocidad. Por tanto, una MAN permite que dos nodos remotos se comuniquen como si formaran parte de la misma red de área local. Una MAN está conformada por conmutadores o *routers* conectados entre sí mediante conexiones de alta velocidad (generalmente cables de fibra óptica).

4.2.9.3 Redes WAN: Una WAN (red de área extensa) conecta múltiples LAN entre sí a través de grandes distancias geográficas. La velocidad disponible en una red WAN varía según el costo de las conexiones (que se incrementa con la distancia) y puede ser más reducida. Este tipo de red funciona con *routers*, que pueden "elegir" la

ruta más apropiada para que los datos lleguen a un nodo (punto) de la red. La WAN más conocida es Internet."[7]

4.2.10 Dispositivos de Red: GALINDO, José Fernando en el documento Dispositivos Activos de Red, material objeto de aprendizaje del SENA, presenta la siguiente definición:

"Los dispositivos activos de red son equipos electrónicos que distribuye la banda ancha para conectar cada equipo (Computadores) a una red, esto permite compartir, crear y obtener información. Es necesario conocerlos para poder identificar la arquitectura tecnológica de la organización y así poder realizar el inventario tecnológico.

Entre los dispositivos Activos de Red podemos encontrar:

4.2.10.1 Concentradores (*HUB*): Un concentrador se utiliza para interconectar computadores y otros dispositivos, permitiendo centralizar el cableado. También, llamado "repetidor multipuerto", porque transmite, o repite los paquetes que éste recibe a todos sus puertos, exceptuando por el que lo recibió. Hay que tener en cuenta la regla 5-4-3 que dice: Solo 5 segmentos se pueden unir con 4 concentradores, pero solamente 3 de ellos pueden estar ocupados.

Tipos:

- Pasivos: Los paneles de conexión o los bloques de conexión. Son puntos de conexión y no amplifican o regeneran la señal; éstos no necesitan corriente eléctrica para funcionar.

- Apilables: Cuando un hub se pone uno encima de otro y estos se interconectan automáticamente por medio de un conector, estos conectores existen en la parte superior e inferior del hub.

- Solos: Consiste en una caja con conexiones, no retrasmiten no amplifican, ideal para conexiones donde no superan 12 usuarios.

[7] VIALFA, Carlos. "Tipos de Redes". {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (http://es.ccm.net/contents/257-tipos-de-redes).

- Modulares: Tienen la característica "*port switching*" que se conmuta por medio de *software*, configurando el *hardware* para dividirlo en varios segmentos *Ethernet* y así asignarlos a un puerto o grupo de puertos y dar flexibilidad para la administración del sistema para balancear la carga de trabajo de los segmentos de la red o cambiar a un usuario de un grupo a otro.

4.2.10.2 ***Gateway***: Dispositivo que permite conectar redes por diferentes protocolos y arquitecturas, convirtiendo la información de las tramas del protocolo origen a un protocolo para la red destino.

4.2.10.3 Enrutadores: Dispositivos para conectar redes en la capa tres del modelo OSI y asegurando el enrutamiento de los paquetes entre las redes limitando el tráfico de *brodcasting* proporcionando: control, seguridad y redundancia; éste dispositivo también se puede utilizar como un *firewall.*

Tipos:

- En función del Área

- Locales: Interconectan dos redes por conexión de los medios físicos de ambos router.

- Extensa: Conectan redes distantes.

- De la manera como se actualizan las tablas de encaminamiento (*Routing*):

- Estáticos: ésta se hace manualmente.

- Dinámicos: Es realizada por el *router* de forma automática.

- Según los protocolos:

- *Routing Information Protocol* (RIP): Comunican diferentes sistemas que pertenecen a la misma red lógica. Poseen tablas dinámicas e intercambian información según su necesidad, permitiendo un total de 14 saltos como máximo.

- Exterior *Gateway Protocol* (EGP): Permite conectar dos sistemas. Buscando entre los *routers* el camino desde el origen hasta el destino.

- *Open Shortest Path First Routing* (OSPF): Minimiza el tráfico de enrutamiento, permitiendo autenticar mensajes salientes; poseen una copia de la topología de la red y todas son idénticas, distribuyendo la información al *router* adyacente, debido a que cada uno de ellos construye su propio árbol de enrutamiento.

- Multiprotocolo: utiliza tramas de forma simultánea para diferentes protocolos de Red, enrutándolas a su destino de forma más rápida y con el menor costo. Son catalogados como *router* de segunda generación, ahorrando gastos innecesarios como el tener un *router* por cada protocolo.

- *Brouter (bridging router)*: *Routers* multiprotocolo con las características de un *bridge*. Su funcionamiento es como los *router* con protocolos enrutables, *source routing* y *spanning tree bridging* y protocolos no enrutables.

- *Trouter*: Combinación entre un *router* y servidor de terminales, utilizado para hacer pequeños grupos de trabajo y con conexión a RALs, WANs, *modems*, impresoras, y otros computadores, pero pueden ocasionar una degradación en el tiempo de respuesta.

4.2.10.4 Tarjeta de red. Denominadas adaptadores de red o tarjetas de interfaz de red o NIC, es un periférico que permite la comunicación entre un computador, el cable de red y la red, permitiendo también compartir recursos con otros computadores de una red.

4.2.10.5 *Transceiver*: Conocido como Transceptor, denominado bajo la forma de Transductor, siendo que se encarga de transmitir una Potencia de un punto a otro. Este dispositivo puede ser de tipo Electromagnéticos, Acústico o Mecánicos, que transmiten una señal hacia otro dispositivo, pero con una transformación de medios.

4.2.10.6 *Switch*: Dispositivo de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Tipos:

- Capa 2: Tienen la capacidad de asimilar y apilar direcciones de red de los dispositivos conectados a cada uno de los puntos de los puertos.

- Capa 3: Son dispositivos que integran *routing y switching*, para altas velocidades, determinando el camino con información de la capa de red (capa 3), haciendo validación de integridad del cableado por un *checksum* (control de redundancia), posibilitan la comunicación entre las diversas *VLAN's*, sin la necesidad de utilizar un *router* externo; es más escalable que un *router*, los *switches* sobreponen la función de ruteo encima del *switching*.

- Capa 4: Llamados también *Layer* 3+. Incorporan las funcionalidades de un *Switch* de capa 3, implementa políticas, filtros a partir de informaciones de capa 4 sobre puertos: TCP/UDP, SNMP, FTP, etc.

4.2.10.7 *Firewall*. Llamado cortafuegos, es parte de un sistema de seguridad de una red que se encarga de bloquear el acceso no autorizado entre los diferentes ámbitos de la arquitectura soportados por un conjunto de normas. Se implementan por *hardware* o *software*, o la combinación de ambos.

Tipos:

- De filtrado de paquetes: Realiza un filtrado de paquetes IP, a nivel de red (capa 3 del modelo OSI).

- De la capa de aplicación: Actúa sobre el nivel de aplicación (capa 7 del modelo OSI), como el tráfico HTTP, filtrados por la *URL* que se quiere conectar, también llamado *proxy* que permite conectarse a Internet de forma controlada.

- Personal: Instalado como un *software* en el computador, filtrando entre el computador y el resto de la red.

- Pasarela: Cuando se establece una conexión TCP/IP o UDP, éste implementa mecanismos de seguridad desde una sesión de mayor seguridad hacia una zona de menor seguridad."[8]

[8] GALINDO, José Fernando. "Dispositivos Activos de Red". {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (https://senaintro.blackboard.com/bbcswebdav/

4.2.11 Modelo OSI: De acuerdo al portal visitado y citado se encontró la siguiente definición:

> "Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Es una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.
>
> El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas."[9]

Figura 1.Modelo OSI

Fuente: (GOOGLE SITES, 2017)

---

institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_disp_activos/utilidades/descargable.pdf).

[9] ANÓNIMO, "Definición de Modelo OSI". {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (https://sites.google.com/site/stigestionydesarrollo/recuperacion/desarrollo-1/recuperacion-provisional/5---describir-el-modelo-osi-definicion-utilidad-y-niveles)

La descripción de cada una de las capas se realiza citando textualmente la información encontrada en el sitio oficial de Microsoft, y el cual se referencia al final de la descripción de cada una de las capas del Modelo OSI.

4.2.11.1 Capa 1: “La Capa física, la más baja del modelo OSI, se encarga de la transmisión y recepción de una secuencia no estructurada de *bits* sin procesar a través de un medio físico. Describe las interfaces eléctrica/óptica, mecánica y funcional al medio físico, y lleva las señales hacia el resto de las capas superiores. Proporciona:

- Codificación de datos: modifica el modelo de señal digital sencilla (1s y 0s) que utiliza el equipo para acomodar mejor las características del medio físico y para ayudar a la sincronización entre *bits* y trama. Determina:

- Qué estado de la señal representa un binario 1

- Como sabe la estación receptora cuándo empieza un "momento *bit*"

- Cómo delimita la estación receptora una trama

- Anexo al medio físico, con capacidad para varias posibilidades en el medio:

- ¿Se utilizará un transceptor externo (MAU) para conectar con el medio?

- ¿Cuántos terminales tienen los conectores y para qué se utiliza cada uno de ellos?

- Técnica de transmisión: determina si se van a transmitir los *bits* codificados por señalización de banda base (digital) o de banda ancha (analógica).

- Transmisión en el medio físico: transmite *bits* como señales eléctricas u ópticas adecuadas para el medio físico y determina lo siguiente.

- Qué opciones de medios físicos pueden utilizarse

- Cuántos voltios/db se deben utilizar para representar un estado de señal en particular mediante un medio físico determinado

4.2.11.2 Capa 2: La capa de vínculo de datos ofrece una transferencia sin errores de tramas de datos desde un nodo a otro a través de la capa física, permitiendo a las capas por encima asumir virtualmente la transmisión sin errores a través del vínculo. Para ello, la capa de vínculo de datos proporciona:

- Establecimiento y finalización de vínculos: establece y finaliza el vínculo lógico entre dos nodos.

- Control del tráfico en tramas: indica al nodo de transmisión que "dé marcha atrás" cuando no haya ningún *búfer* de trama disponible.

- Secuenciación de tramas: transmite y recibe tramas secuencialmente.

- Confirmación de trama: proporciona o espera confirmaciones de trama. Detecta errores y se recupera de ellos cuando se producen en la capa física mediante la retransmisión de tramas no confirmadas y el control de la recepción de tramas duplicadas.

- Delimitación de trama: crea y reconoce los límites de la trama.

- Comprobación de errores de trama: comprueba la integridad de las tramas recibidas.

- Gestión de acceso a medios: determina si el nodo "tiene derecho" a utilizar el medio físico.

4.2.11.3 Capa 3: La capa de red controla el funcionamiento de la subred, decidiendo qué ruta de acceso física deberían tomar los datos en función de las condiciones de la red, la prioridad de servicio y otros factores. Proporciona:

- Enrutamiento: enruta tramas entre redes.

- Control de tráfico de subred: los enrutadores (sistemas intermedios de capa de red) pueden indicar a una estación emisora que "reduzca" su transmisión de tramas cuando el *búfer* del enrutador se llene.

- Fragmentación de tramas: si determina que el tamaño de la unidad de transmisión máxima (MTU) que sigue en el enrutador es inferior al tamaño de la trama, un enrutador puede fragmentar una trama para la transmisión y volver a ensamblarla en la estación de destino.

- Asignación de direcciones lógico-físicas: traduce direcciones lógicas, o nombres, en direcciones físicas.

- Contabilidad del uso de la subred: dispone de funciones de contabilidad para realizar un seguimiento de las tramas reenviadas por sistemas intermedios de subred con el fin de producir información de facturación.

Subred de comunicaciones. El software de capa de red externo, debe generar encabezados; para que el software de capa de red que reside en los sistemas intermedios de subred pueda reconocerlos y utilizarlos para enrutar datos a la dirección de destino.

Esta capa libera a las capas superiores de la necesidad de tener conocimientos sobre la transmisión de datos y las tecnologías de conmutación intermedias que se utilizan para conectar los sistemas de conmutación. Establece, mantiene y finaliza las conexiones entre las instalaciones de comunicación que intervienen (uno o varios sistemas intermedios en la subred de comunicación).

En la capa de red y las capas inferiores, existen protocolos entre pares, entre un nodo y su vecino inmediato, pero es posible que el vecino sea un nodo a través del cual se enrutan datos, no la estación de destino. Las estaciones de origen y de destino pueden estar separadas por muchos sistemas intermedios.

4.2.11.4 Capa 4: La capa de transporte garantiza que los mensajes se entregan sin errores, en secuencia y sin pérdidas o duplicaciones. Libera a los protocolos de capas superiores de cualquier cuestión relacionada con la transferencia de datos entre ellos y sus pares.

El tamaño y la complejidad de un protocolo de transporte dependen del tipo de servicio que pueda obtener de la capa de transporte. Para tener una capa de transporte confiable con una capacidad de circuito virtual, se requiere una mínima capa de transporte. Si la capa de red no es confiable o solo admite datagramas, el protocolo de transporte debería incluir detección y recuperación de errores extensivos.

La capa de transporte proporciona:

- Segmentación de mensajes: acepta un mensaje de la capa (de sesión) que tiene por encima, lo divide en unidades más pequeñas (si no es aún lo suficientemente pequeño) y transmite las unidades más

pequeñas a la capa de red. La capa de transporte en la estación de destino vuelve a ensamblar el mensaje.

- Confirmación de mensajes: proporciona una entrega de mensajes confiable de extremo a extremo con confirmaciones.

- Control del tráfico en mensajes: indica a la estación de transmisión que "dé marcha atrás" cuando no haya ningún *búfer* de mensaje disponible.

- Multiplexación de sesión: multiplexa varias secuencias de mensajes, o sesiones, en un vínculo lógico y realiza un seguimiento de qué mensajes pertenecen a qué sesiones.

Normalmente, la capa de transporte puede aceptar mensajes relativamente grandes, pero existen estrictas limitaciones de tamaño para los mensajes impuestas por la capa de red (o inferior). Como consecuencia, la capa de transporte debe dividir los mensajes en unidades más pequeñas, o tramas, anteponiendo un encabezado a cada una de ellas.

Así pues, la información del encabezado de la capa de transporte debe incluir información de control, como marcadores de inicio y fin de mensajes, para permitir a la capa de transporte del otro extremo reconocer los límites del mensaje. Además, si las capas inferiores no mantienen la secuencia, el encabezado de transporte debe contener información de secuencias para permitir a la capa de transporte en el extremo receptor recolocar las piezas en el orden correcto antes de enviar el mensaje recibido a la capa superior.

Capas de un extremo a otro.

A diferencia de las capas inferiores de "subred" cuyo protocolo se encuentra entre nodos inmediatamente adyacentes, la capa de transporte y las capas superiores son verdaderas capas de "origen a destino" o de un extremo a otro, y no les atañen los detalles de la instalación de comunicaciones subyacente. El *software* de capa de transporte (y el *software* superior) en la estación de origen lleva una conversación con *software* similar en la estación de destino utilizando encabezados de mensajes y mensajes de control.

4.2.11.5 Capa 5. La capa de sesión permite el establecimiento de sesiones entre procesos que se ejecutan en diferentes estaciones. Proporciona:

- Establecimiento, mantenimiento y finalización de sesión: permite que dos procesos de aplicación en diferentes equipos establezcan, utilicen y finalicen una conexión, que se denomina sesión.

- Soporte de sesión: realiza las funciones que permiten a estos procesos comunicarse a través de una red, ejecutando la seguridad, el reconocimiento de nombres, el registro, etc.

4.2.11.6 Capa 6. La capa de presentación da formato a los datos que deberán presentarse en la capa de aplicación. Se puede decir que es el traductor de la red. Esta capa puede traducir datos de un formato utilizado por la capa de la aplicación a un formato común en la estación emisora y, a continuación, traducir el formato común a un formato conocido por la capa de la aplicación en la estación receptora.

La capa de presentación proporciona:

- Traducción del código de caracteres, por ejemplo, de *ASCII* a *EBCDIC*.

- Conversión de datos: orden de *bits*, CR-CR/LF, punto flotante entre enteros, etc.

- Compresión de datos: reduce el número de *bits* que es necesario transmitir en la red.

- Cifrado de datos: cifra los datos por motivos de seguridad. Por ejemplo, cifrado de contraseñas.

4.2.11.7 Capa 7. La capa de aplicación actúa como ventana para los usuarios y los procesos de aplicaciones para tener acceso a servicios de red. Esta capa contiene varias funciones que se utilizan con frecuencia:

- Uso compartido de recursos y redirección de dispositivos
- Acceso a archivos remotos
- Acceso a la impresora remota
- Comunicación entre procesos

- Administración de la red
- Servicios de directorio
- Mensajería electrónica (como correo)
- Terminales virtuales de red”[10]

4.2.12 *MPLS (Multiprotocol Label Switching)*. Para dar una descripción amplia acerca de La conmutación de etiquetas Multiprotocolo (MPLS), se toma como fuente de información el portal Web español 1&1 donde se encuentra un material muy interesante, explicando el tema en detalle, por lo tanto se cita textualmente.

> “MPLS: estándar de transporte de datos en redes. Cuando se habla de transmisión de datos se diferencian fundamentalmente dos tipos. En la transmisión no orientada a conexión, los datos pueden enviarse al sistema de destino desde el terminal que se desee en cualquier momento y sin límite, sin que el camino del paquete tenga que estar definido desde el principio. Cada nodo intermedio (generalmente, *routers*) sabe de forma automática cómo reenviar el flujo de datos. Si bien los servicios no orientados a conexión ofrecen una gran flexibilidad, no aseguran que los recursos necesarios estén efectivamente disponibles.
>
> Por el contrario, en el caso de la transmisión orientada a conexión, el camino de los paquetes de datos se conoce de antemano. Los nodos implicados, generalmente conmutadores, obtienen de la estación que les precede la información necesaria para reenviar los datos hasta que los paquetes llegan al computador de destino al final de la ruta. Este método agiliza en gran medida el largo proceso de enrutamiento propio de los servicios no orientados a conexión. De esta forma, además, se pueden controlar y repartir los recursos de red de una forma óptima. El llamado *Multiprotocol Label Switching (MPLS)* o conmutación de etiquetas multiprotocolo, permite aplicar este método también en redes TCP/IP a pesar de entrar en la categoría de redes no orientadas a conexión.
>
> ¿Qué es el MPLS?: introducción a la conmutación de etiquetas multiprotocolo. A mediados de los años noventa, las grandes redes aún se caracterizaban por una mayor participación de la telefonía frente a la comunicación por datos. En aquel entonces los proveedores de telecomunicaciones operaban redes separadas para

[10] MICROSOFT. “Definición de las siete capas del modelo OSI y explicación de las funciones”. {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (https://support. microsoft.com/es-es/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained)

ambos tipos de transmisión, lo que, por un lado, resultaba en un alto costo financiero y, por el otro, no garantizaba una calidad general del servicio (*Quality of Service, QoS*). Frente a las cualitativamente excelentes redes de voz orientadas a conexión, las redes de datos no orientadas a conexión carecían de la amplitud de banda necesaria. La introducción del protocolo *ATM (Asynchronous Transfer Mode)* pudo resolver esta problemática en su mayor parte, ya que permitía transmitir habla y datos a través de una única infraestructura, pero fue el *Multiprotocol Label Switching (MPLS)* el que ofreció a finales de los 1990 la solución definitiva que permitió utilizar los anchos de banda disponibles de forma eficiente.

Para llevarlo a cabo, MPLS descongestionó unos sistemas de enrutamiento que soportaban una enorme carga: en lugar de dejar que sean las estaciones intermedias las que determinen la mejor ruta del paquete de datos como venía siendo habitual hasta el momento, este método ofrecía la posibilidad de predefinir rutas que establecieran el camino que debía seguir un paquete desde el punto de ingreso *(ingress router)* al punto de egreso *(egress router)*. Las estaciones intermedias (enrutadores de conmutación de etiquetas o *Label Switched Router, LSR*) reconocen esta ruta al examinar las etiquetas con la información de enrutamiento y de servicio asignadas a cada paquete. Esta evaluación tiene lugar con ayuda del hardware adecuado (un conmutador, p. ej.) por encima de la capa de enlace de datos (capa 2 del modelo OSI), mientras que el enrutamiento en el nivel de red (capa 3) desaparece.

Gracias a la extensión Generalized MPLS, esta técnica, originariamente desarrollada solo para redes IP, también está disponible para otros tipos de red como *SONET/SDH (Synchronous Optical Networking / Synchronous Digital Hierarchy) o WSON (Wavelength Switched Optical Network).*

¿Cómo funciona el *Multiprotocol Label Switching*? La intervención del MPLS en redes IP requiere la existencia de una infraestructura lógica y física compuesta por *routers* habilitados para ello. En ellas este método opera de manera preferente dentro de un sistema autónomo (AS): un conjunto de redes IP gestionadas como una unidad y conectadas por al menos un protocolo de puerta de enlace interior (*Interior Gateway Protocol, IGP*). Los administradores de tales sistemas suelen ser proveedores de Internet, universidades o compañías de alcance internacional.

Antes de establecer las rutas, el IGP ha de procurar que todos los *routers* del sistema autónomo puedan encontrarse unos a otros.

Seguidamente se determinan las rutas principales, también llamadas *Label Switched Paths (LSP).* Los mencionados *routers* de ingreso y egreso suelen estar situados en las entradas y las salidas de un sistema y las LSP se pueden activar de manera manual, automática o semiautomática:

- Configuración manual: cada nodo por el que pasa una LSP debe configurarse por separado, procedimiento ineficaz en el caso de grandes redes.

- Configuración semiautomática: solo se deben configurar manualmente algunas estaciones (los tres primeros *hops*, por ejemplo), mientras que el resto de las *LSP* obtiene la información del *IGP*.

- Configuración automática: en este caso es el *IGP* el que define la ruta por completo, aunque sin atender a criterios de optimización.

Los paquetes de datos que se envían dentro de una red MPLS obtienen una cabecera MPLS del *router* de ingreso que se intercala entre los datos de la segunda y la tercera capa en la denominada operación *Push*. Durante la transmisión, cada uno de los nodos implicados en la ruta del paquete (LSR) sustituye (conmuta) la etiqueta por una variante que incluye sus propios datos de conexión (latencia, ancho de banda y *hop* de destino), lo que se denomina a menudo como operación *Swap*. Al final del trayecto la etiqueta se elimina de la cabecera IP (operación *POP*).

Así se compone la cabecera del *Multiprotocol Label Switching*. MPLS amplía la cabecera IP con la llamada MPLS *Label Stack Entry* (pila de etiquetas MPLS), también conocida como MPLS *Shim Header* y que se intercala entre las cabeceras de las capas 2 y 3. Con una longitud de 4 *bytes* (32 *bits*) esta entrada es muy breve, por lo que se puede procesar rápidamente. Esta es su estructura:

32 *bits* de la pila de etiquetas MPLS añaden a un paquete IP estos cuatro datos para el siguiente *hop*:

- *Label* (etiqueta): la etiqueta contiene la información central de la cabecera MPLS, razón por la cual constituye, con 20 *bits*, la parte más larga de la cabecera. Como ya se mencionó, una etiqueta es siempre única y por ello, media únicamente entre dos determinados *routers*. A continuación se edita como corresponde para ser transmitido hacia el siguiente nodo.

- *Traffic Class* (TC): con ayuda de este campo la cabecera informa sobre *Differentiated Services (DiffServ)* y se puede utilizar para clasificar paquetes IP en función de su importancia con el objetivo de garantizar la calidad del servicio: estos 3 bits podrían servir para priorizar a un paquete de datos sobre el resto o para clasificarlo como secundario.

- *Bottom of Stack* (S): este único bit define si la ruta de transmisión más profunda es una ruta simple o está compuesta por varias LSP intercaladas entre sí porque, si este fuera el caso, el paquete estaría marcado por varias etiquetas agrupadas en una pila *(Label stack).* Este campo informa al *router*, en definitiva, de si aún siguen más etiquetas (S=0) o si, por el contrario, la entrada contiene la última etiqueta MPLS de la pila (S=1).

- *Time to live* (TTL): los últimos 8 bits de la entrada muestran la vida útil del paquete de datos definiendo los *routers* que el paquete aún puede recorrer (el límite se sitúa en los 255).

¿Cuál es el papel del MPLS en la actualidad?. En la década de 1990 el MPLS fue de gran ayuda para los proveedores a la hora de desplegar y ampliar sus redes, aunque su mayor velocidad en la transmisión de datos pronto retrocedió a un segundo plano con la entrada en juego de la nueva generación de *routers* de mayor rendimiento con procesador de red integrado. No obstante, hoy sigue siendo utilizado por muchos operadores como método para garantizar la calidad del servicio en el marco de la llamada ingeniería o gestión de tráfico (*Traffic engineering, TE*), un proceso que se ocupa del análisis y la optimización de flujos de datos y en el cual, además de la clasificación de cada conexión de datos, también tiene lugar un análisis del ancho de banda y de la capacidad de cada elemento de red. En función de los resultados de este análisis, la carga de datos se distribuye de la forma más conveniente con el propósito de fortalecer la red entera.

Otro ámbito de aplicación muy extendido de la conmutación de etiquetas multiprotocolo son las redes virtuales privadas o VPN redes aisladas de comunicación que utilizan infraestructuras de red, como Internet, como medio de transporte. Esto permite a los dispositivos conectarse a una red sin que estén físicamente conectados entre sí. Se diferencian básicamente dos tipos de redes virtuales MPLS:

- VPN en la capa 2: las redes privadas en el nivel de enlace de datos pueden ser concebidas para conexiones punto a punto o para el

acceso remoto. Para el usuario de estas VPN, la capa 2 funciona de interfaz para establecer la conexión. Los protocolos básicos son el *Point-to-Point Tunneling Protocol (PPTP)* o *el Layer 2 Tunneling Protocol (L2TP).* De este modo los proveedores de servicios tienen la posibilidad de ofrecer a sus clientes servicios similares a *SDH* y *Ethernet.*

- VPN en la capa 3: estas redes representan para los proveedores de servicios una solución asequible para ofrecer a diferentes clientes (independientemente de los rangos privados de direcciones IP) estructuras de red completamente enrutadas erigidas sobre una única infraestructura IP. La gestión independiente de los clientes mediante etiquetas MPLS individuales y rutas de paquetes predefinidas garantizan la calidad del servicio (los nodos no enrutan en este caso).

Los operadores de grandes redes *WAN (Wide Área Network)* obtienen beneficio de las ofertas de proveedores basadas en MPLS porque, configuradas correctamente, las *Label Switched Paths* optimizan el tráfico de datos y garantizan que todos los usuarios dispongan siempre del ancho de banda que necesitan sin un gran costo. El método también constituye una solución adecuada para redes universitarias internas o para redes corporativas, siempre y cuando se cuente con el presupuesto suficiente.

Ventajas de las VPN con MPLS. La conmutación de etiquetas multiprotocolo compite como tecnología para redes virtuales con la extensión de la pila de protocolos IP IPsec. La actualización de seguridad del protocolo de Internet se caracteriza en especial por sus propios mecanismos de cifrado y su bajo costo, pero la realización de la infraestructura con IPsec no es responsabilidad del proveedor sino del mismo usuario, por lo que, a diferencia del método MPLS, implica más trabajo por su parte. A este respecto el método MPLS ofrece una clara ventaja, pero además se pueden enumerar las siguientes:

- Escaso mantenimiento: operar una red MPLS es responsabilidad del proveedor, como también la configuración IP y el enrutamiento. El cliente se beneficia entonces de una infraestructura acabada, ahorrándose así el esfuerzo de desplegar una red propia.

- Rendimiento excelente: al estar definidas de antemano, las rutas de los datos proveen a la transmisión de una elevada velocidad sometida solo a escasas variaciones. Los acuerdos del nivel de servicio (*SLA, Service Level Agreements*) entre el proveedor y el cliente garantizan

obtener el ancho de banda deseado y un soporte agilizado en caso de fallo.

- Gran flexibilidad: las redes VPN basadas en MPLS garantizan a los proveedores de Internet un amplio margen de maniobra en la cuestión del reparto de recursos, lo que al final también beneficia al cliente. Los proveedores pueden, con este método, acordar paquetes específicos de prestaciones y escalar las redes siempre que se necesite.

- Posibilidad de priorizar servicios: gracias a la infraestructura MPLS, los proveedores pueden ofrecer diferentes niveles de *QoS* porque en ella el ancho de banda alquilado no es estático sino clasificable (*Class of Service*). De esta forma se pueden priorizar algunos servicios como VoIP para garantizar la estabilidad de la transmisión.

¿En qué medida son seguras las redes MPLS?. Las ventajas del MPLS y de las VPN basadas en esta tecnología son especialmente interesantes para empresas e instituciones deslocalizadas que quieren ofrecer a sus clientes acceso a su red. Esto convierte a estas redes en la primera opción cuando se trata de diseñar la infraestructura informática corporativa en estos casos porque permiten a los usuarios conectarse a la red sin requerir una conexión física o direcciones IP públicas y enrutables en Internet.

A una VPN basada en MPLS solo pueden acceder los usuarios que disponen de los datos necesarios para establecer la conexión, pero este hecho por sí solo no convierte a las redes virtuales en inmunes ante un acceso no autorizado. La denominación como “privada” en el caso de las redes virtuales no hace referencia al cifrado o la protección, sino única y exclusivamente al hecho de que las direcciones IP que se utilizan en ella solo son accesibles de forma interna. Si no se cifrara el intercambio de comunicación, toda la información podría ser filtrada fácilmente, si bien la certificación tampoco ofrece una protección absoluta si al tráfico normal de Internet entre la red y las LAN cliente tiene lugar a través del *router* del operador situado en el borde de la red (también llamado *Provider Edge o PE*). A continuación se enumeran algunos de los posibles riesgos implicados en el uso de infraestructuras MPLS:

- Los paquetes MPLS llegan a la VPN equivocada: a menudo hay errores de software y de configuración que pueden hacer que los paquetes IP con etiqueta MPLS abandonen su red VPN y aparezcan en otra. En este caso el *router* ha conducido los paquetes erróneamente a sistemas que no son fiables pero para los cuales

existe una ruta IP. También es posible que los paquetes de datos sean desviados a propósito a otra red VPN con una etiqueta manipulada (*MPLS-Label Spoofing*) si el enrutador de borde los acepta.

- Conexión de un *router* de borde sin permiso: si a la infraestructura MPLS se conectan varias VPN se corre el riesgo de que un *router* de borde se integre en la VPN de otro cliente sin autorización. Esto podría tener el origen en una mala configuración, pero también en un ataque premeditado. Con ello es posible llevar a cabo otros ataques desde la red con gran facilidad.

- La estructura lógica de la red del proveedor permanece a la vista: si un atacante es capaz de acceder a la estructura lógica de la red MPLS que ha desplegado el proveedor de servicios, los ataques al *router* de borde dejan de ser algo improbable, en especial si sus direcciones son visibles.

- Ataque de denegación de servicio en el *router* PE: en su calidad de encrucijada decisiva para las redes, el *router* de borde del operador (PE *router*) es un objetivo especialmente vulnerable a ataques *Denial of Service* que ponen en peligro la disponibilidad del servicio de la VPN. En este contexto serían posibles, por un lado, las actualizaciones continuas del enrutamiento con *EIGRP (Enhanced Interior Gateway Routing Protocol) u OSPF (Open Shortest Path First)* y por el otro la sobrecarga del *router* enviando paquetes pequeños de datos en masa.

Como vemos, toda VPN debería contar con mecanismos de protección que, sumados al cifrado, aseguren a los *routers* de borde del proveedor de ataques externos. En este punto es recomendable la instalación de una zona desmilitarizada entre dos cortafuegos y la utilización de sistemas de supervisión de la red. Por último, la actualización regular del *hardware* y el *software* así como las medidas de seguridad contra ataques físicos a las puertas de enlace deberían formar parte del estándar de protección."[11]

4.2.13 *Hardening*. DE MAYA, David en su blog web dedicado a la Seguridad informática nos presenta la siguiente definición para *Hardening*:

[11] 1&1 DIGITAL GUIDE. . "MPLS: estándar de transporte de datos en redes". {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (https://www.1and1.es/digitalguide/servidores/know-how/mpls-que-es-el-multiprotocol-label-switching/)

"(palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando *software*, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchos otros métodos y técnicas. Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias ante un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad. Una de las primeras cosas que hay que dejar en claro del *Hardening* es que no necesariamente logrará forjar equipos "invulnerables".

Como conclusión, el *Hardening* es una ayuda indispensable para ahorrarse bastantes dolores de cabeza por parte de los administradores de sistemas. Entre sus ventajas, se puede contar la disminución por incidentes de seguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas, ya que muchas de las posibles causas de ellos quedarán descartadas en virtud de las medidas tomadas, y finalmente la posibilidad de poder hacer un seguimiento de los incidentes y en algunos casos identificar el origen de los mismos.

Es muy importante entender que un buen *hardening* a nivel de red podría evitar o disminuir el daño que podría hacer un atacante dentro de ella, es decir no es lo mismo tener los sistemas "abajo" (todo el conjunto); que solo tener un único servicio aislado o caído; se sufrirán perdidas económicas, pero no serán tan catastróficas como perder todo el centro de procesamiento de datos.

Como se menciona anteriormente tener una red completamente impenetrable, es imposible, ya que las redes están creadas, gestionadas por humanos y por lo tanto hay un margen de error que se puede materializar, pero lo que se debe buscar siempre es hacer más difícil a un "ciberdelincuente", la penetración a los sistemas propios o el acceso al centro de procesamiento de datos."[12]

[12] DE MAYA, David. "Hardening de nuestro Centro de Datos". {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (https://hardsoftsecurity.es/hardeningDeNuestro Centro DeDatosv2.pdf)

4.3 MARCO CONTEXTUAL

La información referente al marco contextual de la E.S.E Hospital Santa Mónica, se toma textualmente de la página Web Institucional http://www.hospitalsantamonica.gov.co/

4.3.1 "Quienes somos. Somos una Empresa Social del Estado que brinda atención en salud en diferentes niveles de complejidad, ubicada en Dosquebradas, municipio industrial por excelencia, perteneciente al paisaje cultural cafetero, declarado por la UNESCO patrimonio cultural de la humanidad constituyéndose en un lugar privilegiado del territorio Colombiano por su accesibilidad (paso obligado a los principales centros del país al estar enmarcada entre los departamentos de Antioquia, Caldas, Tolima, Valle, Quindío y Chocó) y por su connotación dentro del Paisaje Cultural Cafetero.

Nos distinguimos de las demás empresas del sector, por la gestión realizada en torno al mejoramiento de la calidad de nuestros servicios lo que nos posicionó entre los 10 mejores en el Banco de Éxitos de la Administración Pública a nivel nacional, por la rentabilidad económica y social generada y por la inversión que se realiza para mejorar las condiciones físicas, tecnológicas y científicas.

Nuestros servicios tienen como objetivo, satisfacer las necesidades y expectativas en salud y bienestar de la población del área de influencia, de pacientes particulares y de otros municipios que demandan nuestros servicios.

Nuestros clientes son los usuarios directos que solicitan particularmente los servicios o los intermediarios que son los administradores de planes de beneficios como EPS´s, aseguradoras, el departamento y el municipio.

4.3.2 Misión. Somos una Empresa Social del estado que presta servicios de salud de baja y mediana complejidad en la sede principal y centros de atención ambulatoria, con calidad, seguridad, respeto y calidez humana, comprometidos con el mejoramiento continuo y la sostenibilidad financiera, contamos con tecnología apropiada y talento humano competente que contribuye a la formación de profesionales de la salud.

4.3.3 Visión. Para el 2020 seremos una empresa líder en salud, acreditada reconocida por la excelencia y seguridad en la prestación de sus servicios, a través de la innovación y reconocimiento del portafolio de servicios, tecnología e infraestructura cómoda y segura, con un sistema de información integral y oportuna, autónoma y económicamente sostenible.

4.3.4 Valores Institucionales

- Humanización: Brindamos una servicio amable, teniendo en cuenta todas las necesidades del usuario en lo físico, emocional y espiritual.

- Respeto: Brindamos una atención que busca no causar ofensa ni perjuicio al usuario.

- Tolerancia: Aceptamos las opiniones, ideas o actitudes de nuestros usuarios.

- Equidad: Brindamos una atención justa e igualitaria a los usuarios de acuerdo con sus necesidades, independientemente de su estrato socioeconómico, filiación política, raza, sexo, edad, religión o condiciones físicas.

- Solidaridad: Ayudamos y ponemos nuestras capacidades al servicio de nuestros usuarios.

4.3.5 Principios Institucionales

- Ética: Trabajamos bajo una conducta moral haciendo las cosas bien, siendo coherentes entre el actuar y el pensar.

- Responsabilidad: Cumplimos con las obligaciones y tenemos cuidado especial en la toma de decisiones.

- Calidad: Contamos con un sistema de gestión que busca el mejoramiento continuo con el fin de satisfacer las necesidades del cliente interno y externo.
- Seguridad del paciente: Trabajamos para prevenir la ocurrencia de situaciones que afecten la integridad del usuario y reducir la ocurrencia de eventos adversos en la atención en salud.

- Rentabilidad: Tenemos la capacidad de generar beneficios adicionales sobre la inversión.

- Sentido de pertenencia: Nos sentimos parte de la institución aportando a su cuidado y orden.

4.3.6 Organigrama

Figura 2. Organigrama Institucional

Fuente: (HOSPITAL SANTA MÓNICA, 2017)

4.3.7 Portafolio de Servicios Consulta y Atención Especializada

- Medicina y odontología general
- Programas de Promoción y Prevención (PyP)
- Programas Crónicos
- Trabajo Social
- Radiología
- Anestesiología
- Cardiología
- Dermatología
- Gastroenterología
- Ginecología
- Pediatría
- Medicina Interna
- Medicina de Familiar
- Oftalmología

- Urología
- Ortopedia
- Otorrinolaringología

Salud Oral Especializada

- Odontopediatría
- Cirugía Maxilofacial
- Endodoncia
- Rehabilitación Oral

Laboratorio

- 24 horas 1 y 2 nivel
- Hematología y coagulación
- Química
- Pruebas especiales
- Microscopia
- Microbiología
- Servicio Transfusional
- Uroanálisis y frescos

Cirugía Laparoscópica

- De tórax
- Ginecológica
- Urológica

Paquetes Quirúrgicos

- Cirugía General
- Cirugía Pediátrica
- Dermatología
- Gastroenterología
- Urología
- Ginecología y Obstetricia
- Oftalmología
- Ortopedia Otorrinolaringología

Terapias y Rehabilitación

- Rehabilitación Cardiaca
- Rehabilitación De Piso Pélvico

- Rehabilitación Respiratoria
- Rehabilitación De Lenguaje
- Rehabilitación Física
- Terapia De Salud Ocupacional
- Trabajo Social

Convenios con EPS y EAPB

- Alcaldía de Dosquebradas
- Gobernación de Risaralda
- Asmetsalud
- Medimas
- Pijaos Salud (EPS Indígena)
- EPS Sanitas
- EPS Sura
- SOS
- Cosmitet
- Seccional de Sanidad
- Fiduprevisora (Inpec)"[13]

4.3.8 Descripción General

- La E.S.E Hospital Santa Mónica en la actualidad cuenta con una sede principal, y 6 puestos de salud conectados a la sede principal por medio de un servicio de transmisión de datos contratado con un operador de la región, lo que les permite tener acceso a cada una de las aplicaciones institucionales y trabajar en línea con la sede principal.

- En la sede principal se cuenta con un gabinete central de datos y de allí se desprenden 5 enlaces en fibra para igual número de gabinetes secundarios, los cuales a su vez alimentan otra serie de gabinetes, para contar con un total de 10 gabinetes de datos descentralizados; ubicados en diferentes áreas de la institución.

- En la institución se cuentan actualmente con alrededor de 300 equipos de cómputo conectados a la red de datos, entre equipos propios de la institución y equipos pertenecientes a los outsourcing, que operan dentro del hospital, de acuerdo a las necesidades de los servicios.

[13] INSTITUCIONAL. "Sitio Web E.S.E. Hospital Santa Mónica". {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (http://www.hospitalsantamonica.gov.co/quienessomos)

- La entidad tiene implementado un servicio de VPN por medio del cual se conectan, desde los diferentes consultorios médicos de especialistas al aplicativo de historia clínica de la institución, con el fin de consultar y registrar la información correspondiente a la consulta médica.

- Cuenta con un servicio de internet de 30 MB, el cual es compartido y administrado por medio de un proxy sobre Windows con los diferentes equipos pertenecientes a la institución.

- El área de sistemas de información está compuesta por cinco personas las cuales se distribuyen en la Coordinadora del área que se encarga de la gestión administrativa, un técnico de sistemas que se encarga del soporte técnico de hardware y redes, apoyado a su vez por un auxiliar administrativo en dichas funciones, un ingeniero de sistemas encargado de la generación de información y desarrollo de aplicaciones de uso institucional y finalmente por un ingeniero de sistemas que se encarga del soporte a los aplicativos de uso institucionales.

4.4 MARCO LEGAL

4.4.1 "Resolución de la CRC 2258 de 2009. Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información".[14]

4.4.2 "Ley 599 de 2000: Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y

[14] MINISTERIO DE LA TECNOLOGÍA, INDUSTRIA Y COMERCIO. Lineamientos de política para ciberseguridad y ciberdefensa. {En línea}. {Consultado el 07 de Noviembre de 2017} disponible en: (https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf)

se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa".[15]

4.4.3 "Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".[16]

"Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos

[15] Ibíd p. 10.
[16] Ibíd p. 11.

informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269 F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO

De las atentados informáticos y otras infracciones

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad."[17]

4.4.4 "Resolución número 1995 de 1999: Por la cual se establecen normas para el manejo de la Historia Clínica EL MINISTRO DE SALUD En ejercicio de las facultades legales y en especial las conferidas por los artículos 1, 3, 4 y los numerales 1 y 3 del artículo 7 del Decreto 1292 de 1994 y CONSIDERANDO Que conforme al artículo 8 de la Ley 10 de 1990, al Ministerio de Salud le corresponde formular las políticas y dictar todas las normas científico-administrativas, de obligatorio cumplimiento por las entidades que integran el sistema de salud. Que la Ley 100 de 1993, en su Artículo 173 numeral 2, faculta al Ministerio de Salud para dictar las normas científicas que regulan la calidad de los servicios, de obligatorio cumplimiento por parte de todas las Entidades Promotoras de Salud, los Prestadores de Servicios de Salud del Sistema General de Seguridad Social en Salud y las direcciones Seccionales, Distritales y Locales de Salud.

Que el Decreto 2174 de 1996, mediante el cual se organizó el Sistema Obligatorio de Garantía de Calidad del Sistema General de Seguridad Social en Salud, en el numeral 4 del Artículo 5, estableció como uno de los objetivos del mismo, estimular el desarrollo de un sistema de información sobre la calidad, que facilitara la realización de las labores de auditoría, vigilancia y control y contribuyera a una mayor información de los usuarios. Que la Historia Clínica es un documento de vital importancia para la prestación de los servicios de atención en salud y para el desarrollo científico y cultural del sector.

Que de conformidad con el Artículo 35 de la Ley 23 de 1981, corresponde al Ministerio de Salud implantar modelos relacionados con el diligenciamiento de la Historia Clínica en el Sistema Nacional de Salud. Que se hace necesario expedir las normas correspondientes al diligenciamiento, administración, conservación, custodia y confidencialidad de las historias clínicas, conforme a los

[17] DELTA. "Ley de Delitos Informáticos en Colombia". {En línea}. {consultado el 07 de Noviembre de 2017} disponible en: (http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia)

parámetros del Ministerio de Salud y del Archivo General de la Nación en lo concerniente a los aspectos archivísticos contemplados en la Ley 80 de 1989."[18]

4.4.5 "Resolución 839 de 2017: Custodia - Conservación – Disposición Final de expedientes clínicos (Registros Asistenciales)

La Resolución 839 de 2017 modifica parcialmente la Resolución 1995 de 1999 (por la cual se establecen normas para el manejo de la Historia Clínica), generando directrices en cuanto al manejo de los registros asistenciales (custodia, conservación y disposición final); a continuación se relacionan aspectos importantes:

La conservación ya no será durante veinte (20) años, sólo será de quince (15) años; 5 años en archivo de gestión y diez (10) años en archivo central; en casos de violaciones a los derechos humanos la retención y conservación del expediente clínico se duplicará.

Luego de cumplidos los plazos anteriores y previa disposición final, deberá publicarse como mínimo dos (2) avisos en un diario oficial de amplia circulación, con espacio entre una publicación y otra de ocho (8) días; la información deberá establecer claramente el tiempo para que el usuario o representante legal reclame su historia clínica (dicho plazo podrá ampliarse hasta por dos meses más).

Podrá realizarse la disposición final, siempre y cuando se cumplan con las siguientes condiciones:

Haber cumplido con los tiempos de retención y conservación.

Que se haya realizado la publicación en diario oficial de amplia circulación, según lo descrito anteriormente.

Realizar una revisión de cada expediente, descartando que no tenga valor científico, histórico o cultural.

Cada historia clínica a eliminar, deben estar relacionadas en un acta de eliminación, en la cual deberá consignarse la siguiente información.

[18] MINISTERIO DE SALUD. "Resolución número 1995 de 1999". {En línea}. {07 de Noviembre de 2017} disponible en: (https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995 %20DE%201999.pdf)

Diligenciar documento Formato Único de Inventario Documental, propuesto por el Archivo General de la Nación. Dicha información deberá publicarse en un medio de amplia difusión o en su página de internet.

En caso de liquidación de una institución o cierre de un servicio, para la entrega de los registros asistenciales, deberá tenerse en cuenta:

Publicar como mínimo dos (2) avisos en un diario oficial de amplia circulación, con espacio entre una publicación y otra de ocho (8) días; la información deberá establecer claramente el tiempo para que el usuario o representante legal reclame su historia clínica (dicho plazo podrá ampliarse hasta por dos meses más).

En caso de no poderse realizar la entrega del expediente clínico, al paciente o responsable, deberá levantarse un acta con los datos de quienes no las recogieron y se remitirá con la historia clínica a la Empresa Promotora de Salud – EPS; del acta levantada deberá remitirse una copia a la entidad Departamental o Distrital de Salud.

Cuando el paciente no se encuentre afiliado a una EPS, los registros asistenciales deberán entregarse y relacionados en acta a la entidad Distrital o Territorial de Salud; este mismo proceso deberá ser realizado por los herederos en caso de fallecimiento del profesional tratante."[19]

[19] ACTUALISALUD. "Resolución 839 de 2017". {En línea}. {Consultado el 07 de Noviembre de 2017} disponible en: (http://www.actualisalud.com/index.php/usuarios-registrados-online/379-resolucion-839-de-2017)

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

Es un proyecto aplicado de conocimiento cuyo principal propósito es la solución de un problema en particular, para este caso se intervendrá la infraestructura de redes de datos de la E.S.E. Hospital Santa Mónica, con el fin de identificar debilidades, vulnerabilidades y riesgos, que puedan afectar la seguridad de la información de la institución.

Después de identificar las debilidades, riesgos y vulnerabilidades, se pasará a realizar una serie de recomendaciones a la institución, en aras de sensibilizar y crear conciencia de los riesgos a los que se encuentra expuesta la infraestructura de redes de datos, para que tomen las medidas que crean necesarias en pro de la mitigación de los hallazgos encontrados.

De acuerdo al desarrollo del proyecto aplicado se formularan una serie de actividades enfocadas al área objeto de estudio, como lo es la infraestructura de la red de datos de la institución, procurando que estas vayan encaminadas hacia la consecución del objetivo principal del proyecto; haciendo uso de las diferentes técnicas de recolección de información que serán descritas más adelante.

5.2 ALCANCE DEL PROYECTO

El presente proyecto se aplicará específicamente sobre la infraestructura de la red de datos de la E.S.E. Hospital Santa Mónica, se identificarán las debilidades y riesgos asociados, que puedan afectar la seguridad de la información de la institución, y posteriormente se entregará una serie de recomendaciones con el fin que la institución tome conciencia, y emprenda las medidas necesarias para la mitigación de los hallazgos en beneficio de la Seguridad de la información institucional.

5.3 RECOLECCIÓN DE INFORMACIÓN

Con el propósito de recopilar la información necesaria para el desarrollo del presente proyecto, se hará uso de los diferentes tipos de recolección que se describen a continuación; con el fin de identificar las posibles debilidades y riesgos a los que se encuentra expuesta la infraestructura de la red de datos a intervenir.

5.3.1 Recolección Física. Se realizará una inspección a los entornos físicos donde se encuentran ubicados los diferentes componentes de la red de datos, por medio de esta se pretende detectar mediante la observación directa que debilidades, riesgos y vulnerabilidades se pueden presentar y afectan directamente la infraestructura objeto de estudio.

5.3.2 Encuesta: se realizará una encuesta, que consolidan una serie de preguntas dirigidas, a los responsables del área de sistemas de información, y las cuales están enfocadas a diagnosticar, el estado actual de las redes de datos de la institución, con el fin de obtener la mayor información, para el desarrollo del presente proyecto.

5.3.3 *Ethical Hacking y Pentesting*: se realizarán pruebas de *hacking* ético apoyados en herramientas de *software* libre, con el objetivo de identificar posibles vulnerabilidades y riesgos presentes en la red de datos de la Entidad.

5.4 TRATAMIENTO DE LA INFORMACIÓN

En esta fase se realiza la consolidación y tabulación de la información recolectada, mediante la aplicación de las diferentes técnicas. Estos datos serán agrupados y procesados, haciendo uso de herramientas disponibles en la hoja de cálculo de Excel (tablas dinámicas, macros, graficas, entre otras), de tal manera que los resultados arrojados permitan realizar un análisis adecuado; el cual es el insumo principal para la generación de las recomendaciones, que se conferirán a la Coordinación de Sistemas, de tal manera que sean evaluadas y puestas en práctica de acuerdo a sus criterios de priorización, pero siempre enfocadas hacia la consecución de los objetivos propuestos.

5.5 METODOLOGÍA DE DESARROLLO

Después del análisis de diferentes métodos para la implementación de Sistemas de Gestión de Calidad, se pudo evidenciar, que la herramienta más recomendada es la aplicación del ciclo PHVA (Planear – Hacer – Verificar - Actuar), el cual es un ciclo lógico que además de la implementación, permite el fortalecimiento y sostenimiento del sistema de gestión, inmerso siempre en la mejora continua.

Teniendo en cuenta, que el alcance del presente proyecto es de identificar (Debilidades y riesgos), y recomendar (Acciones de mejora); solo se ejecutarán los ciclos de planeación y ejecución, ya que la verificación y acción le

corresponderá a la institución, cuando se implementen las acciones propuestas y realicen el seguimiento correspondiente.

5.5.1 Planear. Esta etapa es vital en el desarrollo del proyecto, debido a que de aquí se deriva la viabilidad del mismo, por lo tanto, en esta etapa se pueden identificar las siguientes actividades:

- Obtener la aprobación por parte del área directiva de la organización objeto de estudio, aval que ya se encuentra oficialmente firmado por la Gerencia de la Institución y la Coordinadora del área de Sistemas de Información.

- Definir el alcance del desarrollo del trabajo de grado, el cual se encuentra delimitado dentro del planteamiento de los objetivos y la metodología de la investigación.

- Realizar el inventario de activos correspondientes a la infraestructura de la red de datos de la Institución.

- Levantar la información correspondiente, haciendo uso de las diferentes técnicas de recolección definidas para el desarrollo del proyecto.

- Selección de las herramientas de monitoreo basadas en *software* libre.

5.5.2 Hacer. En esta etapa como su nombre lo describe se debe iniciar con las implementaciones correspondientes, basadas en las directrices y hallazgos encontrados en la planeación, por lo tanto, aquí se debe realizar las siguientes actividades:

- Identificar las debilidades, riesgos y vulnerabilidades que afectan directamente los componentes que hacen parte de la infraestructura de la red de datos de la Institución.

- Entregar a la Coordinación de Sistemas las recomendaciones y resultados del proyecto.

6. DESARROLLO DEL PROYECTO

6.1 INVENTARIO DE ACTIVOS DE RED DE DATOS

De acuerdo a la información suministrada por el personal del área de sistemas, y corroborado con la inspección física que se realizó a cada uno de los gabinetes de Red de datos con los que cuenta la institución, se logró identificar cada uno de los activos de red que serán objeto de estudio en el presente trabajo, por lo tanto dicho consolidado se presenta a continuación:

Tabla 1. Dispositivos Activos de Red

UBICACIÓN - RACK	MARCA	MODELO	No. PUERTOS
PRINCIPAL	HP	HP V1910-48G	48
	HP	HP V1910-24G-PoE	24
	3COM	Baseline Switch 2024	24
	3COM	Switch 3300 XM 24	24
	3COM	Gigabit Switch 3CGSU08	8
	HUAWEY	QUIDWAY S2300 SERIES (UNE)	8
	FORTINET	FORTIGATE 50B (UNE)	4
CONSULTA EXTERNA	3COM	Baseline Switch 2824 SFP Plus	24
	3COM	Baseline Switch 2024	24
	HP	HP V1910-24G	24
LABORATORIO	HP	HP 1920-24G	24
SIAU	3COM	Baseline Switch 2952-SFP PLUS	48
URGENCIAS	3COM	Baseline Switch 2824-SFP Plus	24
	3COM	Baseline Switch 2024	24
MANTENIMIENTO	CISCO	SF300-24	24
CLINICA ODONTOLÓGICA	HP	HP 1920-48G	48
FISIOTERAPIA RITA ARANGO	CISCO	SF200-24	24
	TP-LINK	TL-SG1008D	16

Tabla 1. (Continuación)

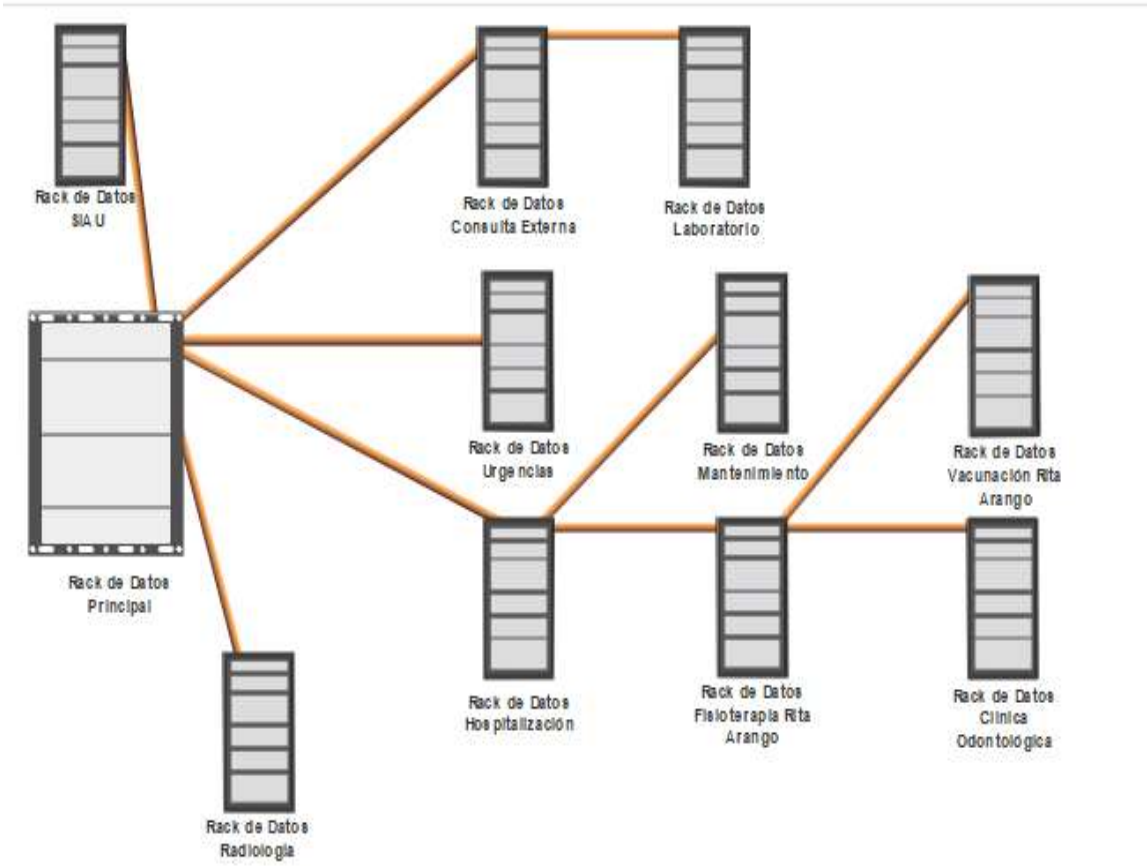
UBICACIÓN - RACK	MARCA	MODELO	No. PUERTOS
VACUNACIÓN RITA ARANGO	QPCOM	QP-524X	24
HOSPITALIZACIÓN	3COM	Baseline Switch 2824-SFP Plus	24
	3COM	Baseline Switch 22024	24
RADIOLOGÍA	HP	HP 1920 series Switch	24
OFICINA SISTEMAS	TPLINK	ROUTER	4
OFICINA DE GERENCIA	TPLINK	ROUTER	4
PUESTO DE SALUD BALSO	Hewlett Packard	Enterprise	48
	HUAWEY	HG8245H (UNE)	4
PUESTO DE SALUD JAPÓN	ENCORE	Nway Switch	16
	Speedtouch	Thomson ST546 V6 (UNE)	4
PUESTO DE SALUD FRAILES	3COM		24
	Speedtouch	Thomson ST546 V6 (UNE)	4
PUESTO DE SALUD SANTA TERESITA 1er PISO	Hewlett Packard	Hp 1920-24g	24
PUESTO DE SALUD SANTA TERESITA 2do PISO	3COM	Baseline Switch 2024	24
	HUAWEY	HG532e (UNE)	4
PUESTO DE SALUD VILLA CAROLA	Hewlett Packard	Hp 1410-16	16
	Mikrotik	RouterBoard 750 (UNE)	6
PUESTO DE SALUD BADEA	ENCORE	Nway Switch	8
	Speedtouch	HG532e (UNE)	4

Fuente: autor

6.2 INFRAESTRUCTURA DE RED DE DATOS INSTITUCIONAL

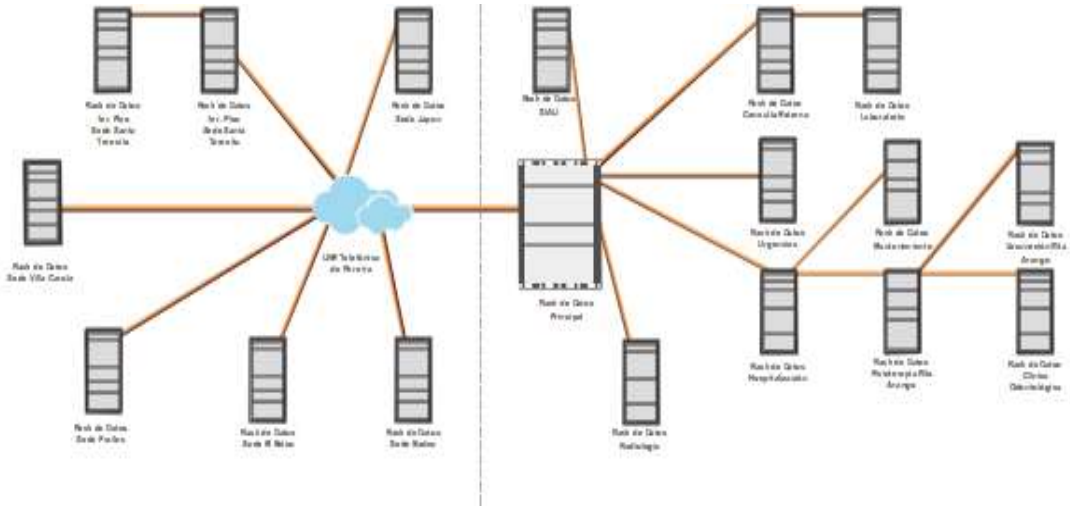
Los diagramas que se presentan a continuación fueron elaborados completamente por autor, basado en el recorrido realizado por cada uno de los Gabinetes que componen la Red de datos de la Sede Principal y por cada uno de los Puestos de Salud, para identificar de primera mano, en términos generales como es su infraestructura, y el tipo de conexión existente entre cada uno de los puntos remotos con la Sede Principal

Figura 3. Diagrama General de Gabinetes Sede Principal



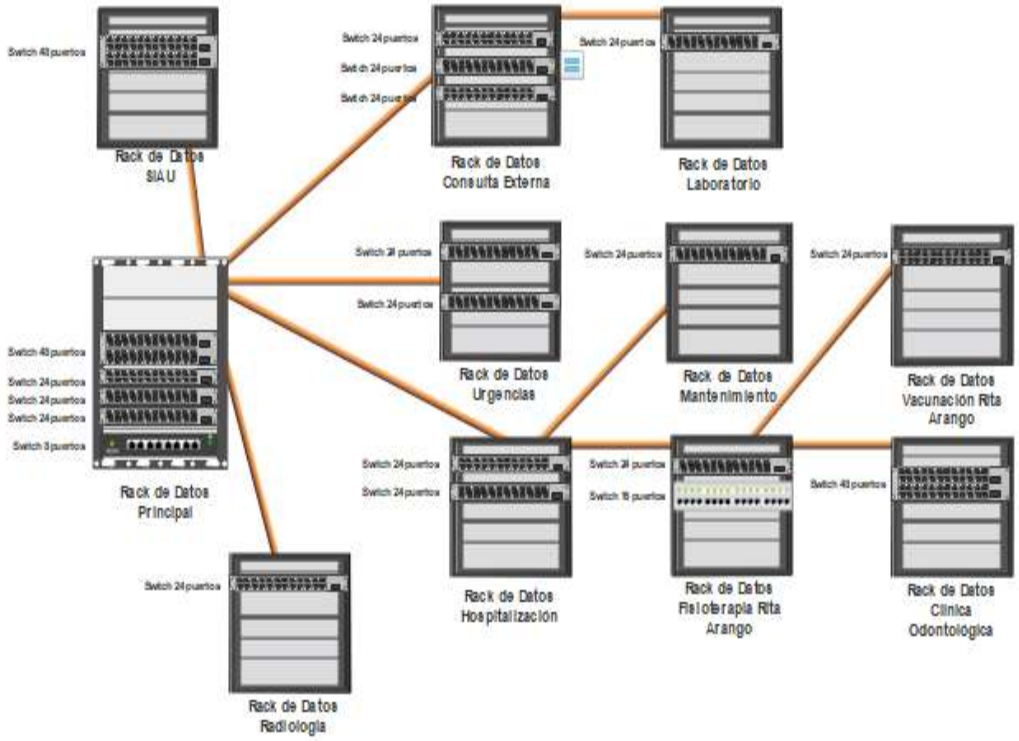
Fuente: autor

Figura 4. Diagrama general Gabinetes Sedes Ambulatorias



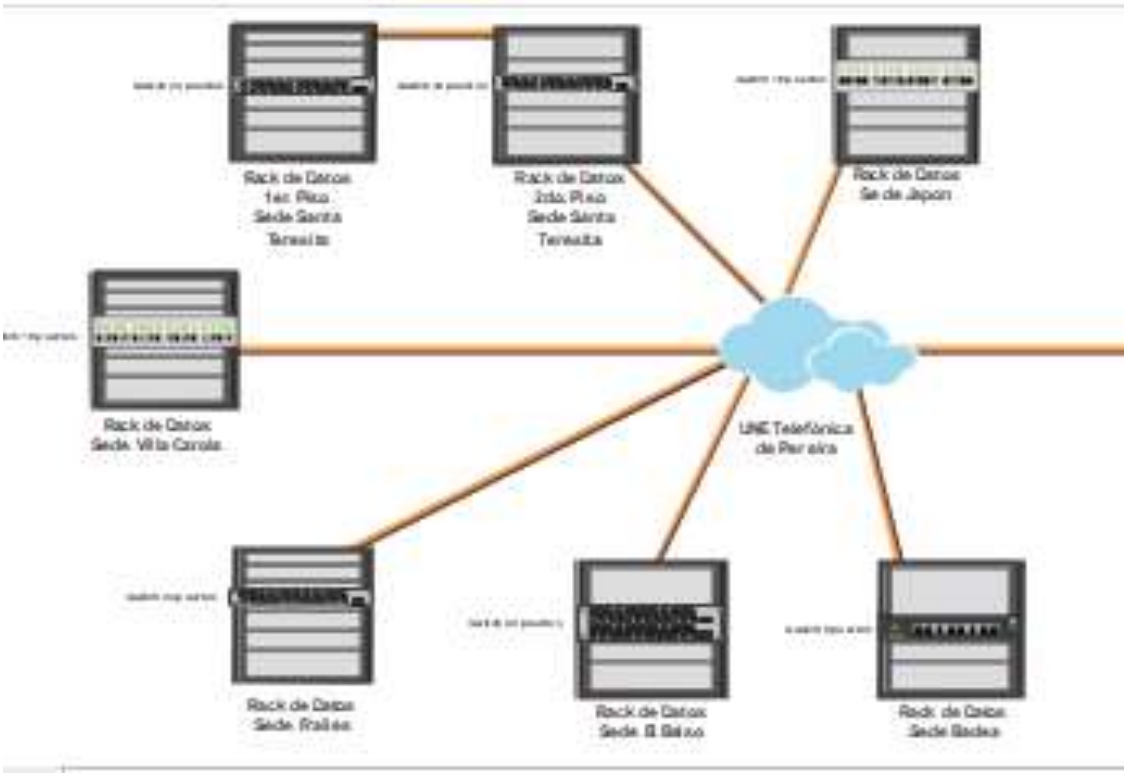
Fuente: autor

Figura 5. Diagrama General de Gabinetes con Dispositivos de Red Sede Principal



Fuente: autor

Figura 6. Diagrama General de Gabinetes con Dispositivos de Red Sedes Ambulatorias



Fuente: autor

6.3 RECURSO HUMANO ÁREA DE SISTEMAS DE INFORMACIÓN

Tabla 2. Recurso Humano Área de Sistemas

CARGO	PERFIL	FUNCIONES GENERALES
Coordinadora de Sistemas de Información y Gestión documental	Tecnóloga en Sistemas Auditora en Sistemas de Gestión de Calidad Personal de Planta Experiencia Sector Salud 23 años	Coordinar el área de sistemas de información, Archivo y Gestión documental. Liderar los procesos de calidad de las áreas que coordina. Documentación y seguimiento a los diferentes procesos implementados en el Sistema Gestión de Calidad de la Institución (Institución Certificado por la ISO 9001, desde el año 2004).
Ingeniero de Soporte	Ingeniero de Sistemas Especialista en Gestión de Proyectos Contratista Externo Experiencia Sector Salud 26 años	Desarrollo y mantenimiento de aplicaciones institucionales. Generación de Información para presentación ante los diferentes organismos que lo requieran.
Ingeniero de Soporte	Ingeniero de Sistemas Contratista Experiencia Sector Salud 12 años	Administrador de base de datos de producción Institucional. Soporte a aplicativos administrativos y asistenciales CNT. Apoyo en validación y envío de los diferentes informes enviados a los órganos de control.
Técnico	Tecnólogo de Sistemas Especialización tecnológica en bases de datos Outsourcing Temporal de Personal Experiencia Sector Salud 4 años	Administrador de Red Soporte a Usuarios en demás aplicativos de uso específico Apoyo en publicación Portal Web. Mantenimiento preventivo y correctivo de Hardware y Software
Auxiliar de Sistemas	Técnico de Sistemas Outsourcing Temporal de Personal Experiencia Sector Salud 5 meses	Apoyo en soporte técnico a usuarios. Apoyo Mantenimiento preventivo y correctivo de Hardware y Software

Fuente: autor

6.4 RECOLECCIÓN DE INFORMACIÓN

6.4.1 Entrevista Personal del área de Sistemas de Información: La entrevista fue atendida por el Técnico de Sistemas Humberto Herrera, quien en la actualidad se encuentra encargado de la administración y Soporte de la Red de datos de la Empresa.

A continuación, se presentarán las preguntas realizadas y las respuestas entregadas por el personal del área de Sistemas de Información.

- ¿La Empresa cuenta con un plano actualizado de la red de datos?

R/= No se cuenta con plano de la red de datos, debido a que en los últimos años la institución ha crecido en todas sus áreas y ha sufrido varias remodelaciones, por lo tanto la instalación del cableado se ha realizado de acuerdo a las necesidades que se presentan. Se tiene el proyecto de actualización y reposición de las redes de datos pendiente desde hace varios años, pero este no se ha podido ejecutar debido a contingencias presupuestales. Se espera que para el próximo año esto se pueda ejecutar, y dejar las redes de datos como deben ser cumpliendo con la normatividad y con la debida certificación. En el Plan Estratégico Institucional desde las últimas cuatro gerencias, se ha incluido el proyecto de Reorganización de la Red de Datos, pero debido a las dificultades presupuestales y financieras, la entidad ha debido priorizar otros proyectos de las áreas misionales trasladando esta actividad a otras gerencias.

- ¿Se cuenta con un inventario actualizado de todos los componentes activos de la Red de datos?

R/= Sí, se tienen identificados los componentes activos de la red de datos (Hojas de Vida).

- ¿De qué categoría es el cableado estructurado de la red de datos instalado actualmente en la Empresa?

R/= El cableado instalado actualmente está en diferentes categorías (5e, 6a y 7a), con el proyecto que le mencione anteriormente se pretende estandarizar el mismo.

- ¿Qué topología presenta la red de datos de la institución?

R/= Como la red de datos ha crecido de manera desorganizada se presenta un hibrido, inicialmente se tenía estipulada una estrella, donde los racks auxiliares se desprendían del rack principal, pero debido al crecimiento de los diferentes

servicios, por lo tanto ha tocado instalar otros racks auxiliares los cuales se han ido conectando al rack más cercano, lo que ha ido generando series de conexiones.

- ¿Cómo se interconectan los diferentes Racks de la red de datos?

R/= En la sede principal, todos estos enlaces se realizaron en Fibra Óptica, solo hay una de las sedes alternas (puesto de salud Santa Teresita), donde dicho enlace se realizó en cable UTP categoría 6a.

- ¿Quién es el encargado de la planificación e instalación de los puntos de red?

R/= Los puntos de red, se van instalando a medida que se va requiriendo para la prestación del servicio, o por aumento en los puestos de trabajo en las diferentes áreas; por lo tanto no hay planificación sino que se responde ante los requerimientos; y la instalación la realiza un contratista externo, con las certificaciones requeridas para la actividad a realizar.

- ¿Cómo se garantiza la calidad de la red de datos?

R/= Cuando se ejecuta un contrato para la instalación de puntos de red nuevos, como requisito se deben entregar dichos puntos certificados, donde se garantice que no hay problemas en el trazo del mismo; adicionalmente aquí no se realiza traslado de puntos de red, si se requiere un punto de red en otra ubicación cercana a los que se encuentra instalados, estos se dejan como están, y se realiza la contratación para la instalación de los puntos de red nuevos.

- ¿La institución cuenta con un plan de mantenimiento para los activos de la red de datos, y con el registro de los mismos?

R/= Sí se cuenta con la programación anual de mantenimiento, aunque estos en ocasiones no se puede cumplir a cabalidad en las fechas establecidas, debido a la criticidad de los servicios; debido a esto se deben concertar para realizarlos en fechas y horarios que la afectación en la prestación de los servicios sea mínima (fines de semana altas horas de la noche o madrugada). Se realiza mantenimiento preventivo (limpieza de Gabinetes y *Switches*), y el registro de los mismos se realiza en los formatos establecidos en el sistema de gestión de calidad como Consolidado de mantenimiento.

- ¿Se cuenta con un plan de actualización de los dispositivos activos de red (*Switches, Routers*)?

R/= No, los dispositivos activos de red, a medida que van llegando se conectan directamente a la red, sin realizar ningún tipo de configuración adicional, y las actualizaciones se han realizado esporádicamente, por parte de los proveedores de dichos dispositivos, cuando han presentado algún tipo de falla, y se reporta por razones de garantía.

- ¿Se tiene segmentada la red de datos de la institución de acuerdo a las diferentes áreas?

R/= No, solo se tiene una red de datos con un solo rango IP, en la sede principal. En cada sede se tiene un direccionamiento IP diferente, pero este es de acuerdo a la configuración que realizo el ISP UNE, a cada uno de los CPE instalados en las sedes; para conectar cada sede alterna (puestos de salud), con la red de datos de la sede principal.

- ¿Se cuenta con alguna herramienta de administración y monitoreo de la red de datos, para detectar fallas en la misma?

R/= No, cuando se presenta alguna falla se realiza de manera empírica, empezando a descartar el área afectada, o identificando los cables de red con un generador de tonos, ya que no se cuenta con el plano de la red; ni tampoco con la totalidad de los puntos de red de datos marcados de la manera adecuada.

- ¿Cómo se interconecta la sede principal con las sedes alternas?

R/= Se tiene contratado con UNE proveedor de servicios de telecomunicaciones de la región, los servicios de internet y Transmisión de Datos, con las diferentes sedes alternas, los cuales de acuerdo a su tamaño y flujo de atención, es el ancho de banda de la conexión. Adicionalmente a esto se tiene instalado un dispositivo Fortinet (Fortigate 50B), suministrado y administrado por el proveedor UNE, para realizar la conexión por VPN, desde los diferentes consultorios médicos de los especialistas, para que de esta manera se puedan conectar al programa de Historia clínica, y registrar en el mismo las atenciones que se realizan desde estos consultorios.

Tabla 3. Conexión Sedes Alternas – Sede Principal

Sede Alterna	Ancho de banda	Tipo de Conexión
Puesto de Salud Santa Teresita	2 MB	Transmisión de Datos (Cobre)
Puesto de Salud Villa Carola	1MB	Transmisión de datos (Radio Enlace)
Puesto de Salud Frailes	2 MB	Transmisión de Datos (Cobre)
Puesto de Salud Japón	1 MB	Transmisión de Datos (Cobre)
Puesto de Salud Badea	1 MB	Transmisión de Datos (Cobre)
Puesto de Salud Balso	1 MB	Transmisión de Datos (Fibra Óptica)
Consultorios médicos especialistas	30 MB	VPN (Internet)

Fuente: autor

- ¿Existe suficiente espacio dentro de las instalaciones donde se encuentran instalados los Rack de la red de datos de forma que permita una circulación fluida?

R/= En el rack principal hay buen espacio para movilizar los elementos y trabajar en ellos, pero en los racks auxiliares, debido a su ubicación y tamaño de los gabinetes se hace muy difícil el acceso a los mismos.

- ¿Existe una adecuada marcación de los Centros que almacenan los Gabinetes de la red de datos?

R/=No se tienen demarcados correctamente los gabinetes que almacenan los dispositivos activos de red y el cableado estructurado, en cada una de las áreas.

- ¿Qué medidas de seguridad se tienen para el acceso a los racks de datos (controles de acceso)?

R/=En el rack principal se tiene restringido el acceso con una chapa de seguridad, y la llave permanece en el área de sistemas; por lo tanto cuando alguien distinto al área requiere acceder, debe diligenciar un formato establecido, donde se indica quien ingresa, persona responsable de la entidad que autoriza el ingreso y que actividad va a realizar, para los demás gabinetes auxiliares se cuenta con llave de la chapa o del gabinete en los casos que se encuentran instalados en áreas abiertas.

- ¿Se cuenta con sistema de cámaras para monitorear el acceso o las zonas aledañas al Rack de datos?

R/=No, aunque la entidad cuenta con CCTV, para monitorear las diferentes áreas las cuales están ubicadas estratégicamente, estas no están ubicadas específicamente para vigilar la seguridad de los gabinetes de datos.

- ¿Se cuenta con sistemas de emergencia, como detectores de Humo, agua, alarmas u otros sensores?

R/=No se cuentan con ninguno de estos elementos, los instalados se encuentran obsoletos o fuera de funcionamiento.

- ¿Los Centros que albergan los gabinetes de la red de datos, cuenta con sistema de refrigeración (aire acondicionado- mini Split)?

R/=En la sede principal solo el Rack Principal, y los Racks de las sedes alternas de Villa Carola, Frailes y Balso; los demás no cuentan con la refrigeración requerida.

- ¿Los dispositivos activos de la red de datos, cuentan con protección ante descargas o fallas eléctricas?

R/=Los dispositivos se encuentran conectados a la red regulada eléctrica de la entidad, igualmente ante la ausencia del fluido eléctrico entra en funcionamiento la planta eléctrica; y el personal manifiesta que se han hecho trabajos de tierras a nivel eléctrico con el fin de protegerse la red eléctrica ante eventuales descargas o cambios bruscos de corriente.

- ¿Se tiene estipulado un plan de contingencia, ante eventuales fallas de la red de datos?

R/=Se tiene establecido en el sistema de gestión de calidad un documento que hace referencia al plan de contingencia del área de sistemas, el cual se encuentra en proceso de actualización, pero allí se evidencia que se debe hacer en los casos donde hay fallas de tipos de red de datos, eléctrico, bases de datos, entre otros.

6.4.2 Visita de inspección física a los gabinetes de la red de datos. Se realiza el recorrido por cada uno de los gabinetes que componen la red de datos de la sede principal y las sedes alternas (Puestos de salud), para verificar el estado y condiciones de las mismas.

SEDE PRINCIPAL. Se detectaron una serie de irregularidades que atentan contra la seguridad de la Infraestructura de la red de datos de la institución, los cuales se enumeraran en los siguientes ítems con la evidencia fotográfica de la misma.

En el rack principal no se cuenta con la respectiva marcación del cableado de red. Lo que no permite identificar cada uno de estos puntos que puesto de trabajo representa.

Figura 7. Marcación Cableado de Red

Fuente. autor

Se puede evidenciar que el Rack no cuenta con Patch Panel donde deben llegar cada uno de los puntos de red cableados, por lo tanto se encuentran ponchados (Conector RJ45) y conectados directamente al Switch, por lo tanto no se cumple la normatividad para el cableado estructurado de Red.

Figura 8. Ponchado de cable de Red

Fuente: autor

Se evidencia que el cableado instalado no llega adecuadamente al Rack de comunicaciones, ya que la canaleta por donde este bajaba se quedó sin la capacidad de albergar todo el cableado de red y fibra que llega a este gabinete, por lo tanto se encuentran expuestos sin ningún tipo de protección.

Figura 9. Cable de Red expuesto

Fuente: autor

Se encuentra una apertura en el techo por donde bajan los cables de red, siendo el material de este removible (Cielo raso), y no se encuentra un cielo firme que se interponga entre el techo y el área de sistemas, por lo tanto esta en inminente riesgo de inundaciones por precipitaciones de agua.

Figura 10. Cielo Raso inadecuado

Fuente: autor

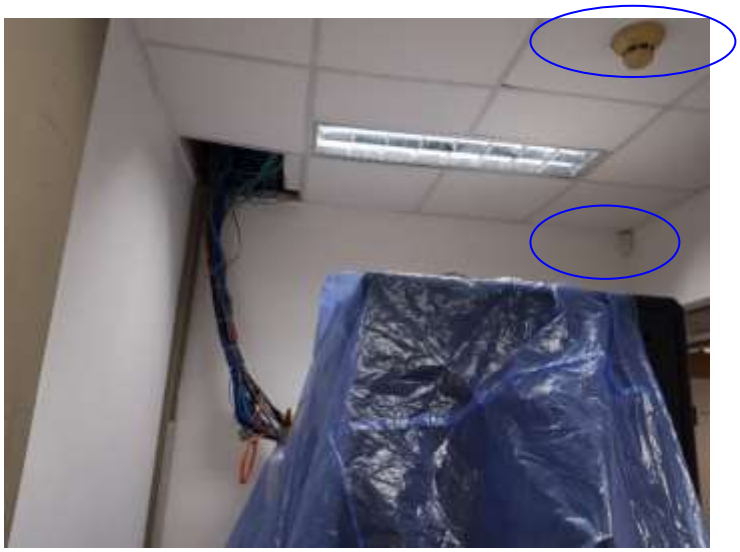
Se evidencia un plástico cubriendo el Rack de comunicaciones y el rack que contiene los Servidores de la Institución, esto con el fin de protegerlos contra el agua que pueda caer sobre ellos. Aunque es una medida que tienen preventiva, no es la adecuada debido a que está generando sobrecalentamiento de cada uno de los dispositivos activos de la red y del centro de datos, limitando la circulación de calor y refrigeración adecuada de cada uno de los dispositivos.

Figura 11. Protección contra el agua inadecuada.

Fuente: autor

Sensores de calor y movimiento instalados, pero sin operación y mantenimiento, por lo tanto estos se encuentran deshabilitados.

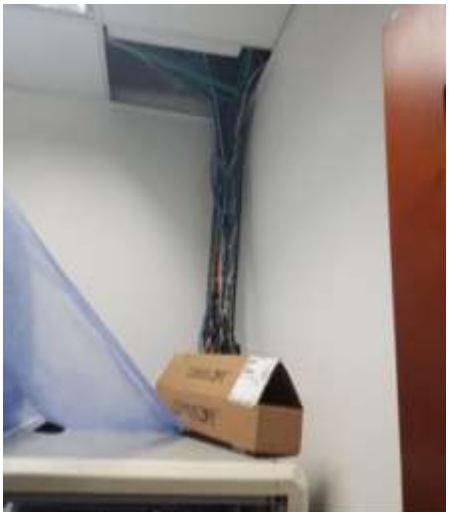
Figura 12. Sensores deshabilitados



Fuente. autor

Objetos de cartón, sobre el gabinete que alberga los diferentes dispositivos activos de red, este siendo un material altamente inflamable no debe estar allí ya que ante un corto que se pueda presentar en el cuarto este material ayudaría a aumentar el riesgo de incendio.

Figura 13. Cartón sobre Rack



Fuente: autor

Dispositivos Activos de red sobrepuestos uno encima del otro, sin tener ningún separador de por medio, lo que evita que haya una correcta circulación del aire entre ellos, lo que conlleva a recalentamiento de los dispositivos lo que puede desencadenar en bajo rendimiento o daño de los mismos

Figura 14. Dispositivos sobrepuestos

Fuente: autor

Enlace entre Racks en fibra, sin las medidas adecuadas de protección, donde se evidencia que se encuentra muy templado lo que puede partir los conectores en el extremo, desencadenando la desconexión del Rack de datos auxiliar con el principal.

Figura 15. Enlace en Fibra sin protección adecuada

Fuente: autor

CENTRO DE ATENCIÓN AMBULATORIA VILLA CAROLA

En el cuarto que alberga el Rack de datos de la sede alterna (Puesto de Salud Villa Carola), se realizaron varios hallazgos; teniendo en cuenta que este es uno de las sedes que menos tiempo tiene de haber sido construida y puesto en funcionamiento.

Aunque dicho cuarto se encuentra sobre el pasillo de circulación e ingreso a la sede se evidencio que el mismo, al momento de la inspección se encontraba abierto, lo que genera que cualquier particular ingrese al mismo, sin ningún tipo de restricción.

Figura 16. Ingreso al cuarto Eléctrico y Comunicaciones Sede Villa Carola

Fuente: autor

El Rack de datos se encuentra mal ubicado, y por lo tanto la puerta del mismo no abre completamente, ya que golpea con el tablero eléctrico instalado en la pared.

Figura 17. Apertura limitada del gabinete de comunicaciones

Fuente: autor

Se encuentra el aire acondicionado que se encarga de enfriar dicho cuarto, en mal estado, se indaga con el personal y refieren que este se encuentra así, desde aproximadamente 3 meses, lo que genera que se presente calentamiento del lugar.

Figura 18. Aire acondicionado fuera de servicio

Fuente: autor

Se evidencia en Rack de datos, Corrosión causado por humedad, lo que indica que en este cuarto así como la humedad afecto este gabinete, de esta misma manera puede afectar algunos de los equipos Activos de la red de datos.

Figura 19. Corrosión causada por humedad

Fuente: autor

CENTRO DE ATENCIÓN AMBULATORIA SANTA TERESITA

En la inspección realizada al puesto de salud de Santa Teresita, se encontró en el Rack de comunicaciones del 2do. Piso, desorden en el mismo y una serie de elementos que no hacen parte de él, como (Planos eléctricos, adaptadores desconectados, dispositivos de red inactivos, cables); y el mismo mostraba signos de no tener una limpieza adecuada.

Figura 20. Desorden Rack de datos 2do. Piso Santa Teresita

Fuente: autor

CENTRO DE ATENCIÓN AMBULATORIA FRAILES

En la visita realizada a la sede de Frailes se realizaron los siguientes hallazgos: la puerta de acceso al Rack de datos se encuentra sobre el pasillo de circulación de los pacientes, y no cuenta con seguro para ingresar al mismo, este permanece ajustado.

Figura 21. Acceso a Rack de Comunicaciones Sede Frailes

Fuente: autor

Se evidencia mucho polvo sobre toda la infraestructura de Rack de Datos y sobre sus dispositivos.

Figura 22. Falta Mantenimiento a Infraestructura de la Red de datos.

Fuente: autor

Aire acondicionado fuera de servicio y muestra de humedad sobre el cielo raso, lo que puede ocasionar afectación sobre los Dispositivos Activos de Red que se encuentran dentro del cuarto.

Figura 23. Aire acondicionado fuera de servicio

Fuente: autor

CENTRO DE ATENCIÓN AMBULATORIA EL JAPÓN

En la inspección al Puesto de salud de Japón se encontró que rack que alberga el cableado y dispositivos activos de la red, es un Gabinete de pared de 5U, el cual no tiene la llave adecuada para asegurarlo, por lo tanto con tan solo halar la

tapa, este se abre, igualmente se evidencia una serie de cables desordenados, sin ningún tipo de marcación y presencia de mucho polvo, al interior del mismo.

Figura 24. Rack de Datos Puesto de Salud Japón, malas condiciones

Fuente: autor

CENTRO DE ATENCIÓN AMBULATORIA LA BADEA

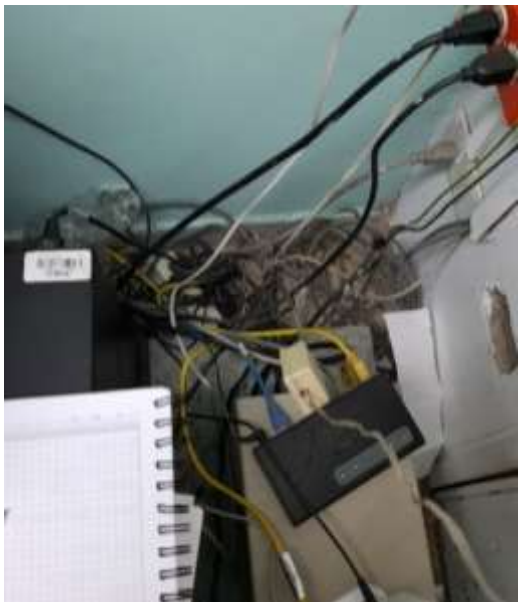
En la visita realizada al puesto de salud de la Badea, se encontraron una serie de condiciones inadecuadas, los cuales afectan directamente la calidad y la prestación de servicio de la red de datos de dicha sede.

- No se cuenta con un gabinete para albergar el cableado de la red de datos y los dispositivos de red.

- No tienen ningún tipo de protección, que los proteja contra daños intencionales, o robo de los dispositivos de red; ya que se encuentra en el área de facturación, el cual es un área abierta donde se puede acceder fácilmente.

- Todos estos dispositivos se encuentran sobre una ups, y se evidencia un enredo de cables de red, con cables eléctricos, lo cual genera ruido en la transmisión.

Figura 25. Dispositivos y Cableado de red, Sede Badea



Fuente: autor

CENTRO DE ATENCIÓN AMBULATORIA EL BALSO

En la visita realizada al puesto de Salud de El Balso, en términos generales se encontraron buenas condiciones, debido a que esta Sede es la más nueva.

Pero se encontró que el personal del aseo estaba almacenando de manera temporal el material de reciclaje en dicho cuarto, lo que atenta contra la integridad del cuarto pues este es material inflamable y allí se puede presentar un corto, debido a que se tiene el rack de comunicaciones y eléctrico.

Figura 26. Material de reciclaje en cuarto que alberga Rack de datos.

Fuente: autor

CENTROS DE DATOS ALTERNOS DE LA SEDE PRINCIPAL

Se finaliza la revisión de los Rack alternos de la Sede Principal, para la verificación de las condiciones de los mismos

- Al visitar El rack de datos del área Consulta Externa, se evidencia un desorden del mismo, sin marcación adecuada del cableado activo e inactivo.

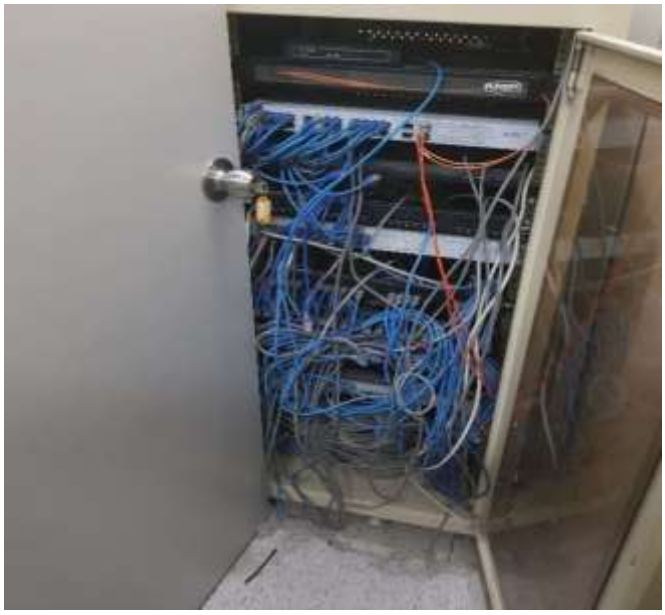
- No se cuenta con la bandeja adecuada para bajar el cableado al Rack.

- No se cuenta con un cielo raso adecuado que brinde la protección al cuarto ante caídas inesperadas de agua por filtración ante las precipitaciones que se presentan en época de lluvias.

- El cuarto se encuentra ubicado sobre un pasillo de circulación, sin la adecuada marcación y chapa de seguridad, lo que puede ocasionar que sin tanto esfuerzo se pueda ingresar al mismo, y cometer daños o robos sobre los activos de red.

- Cuarto muy pequeño que al momento de abrir y cerrar la puerta, se pueden enredar los cables y generar un daño involuntario.

Figura 27. Rack Consulta Externa



Fuente: autor

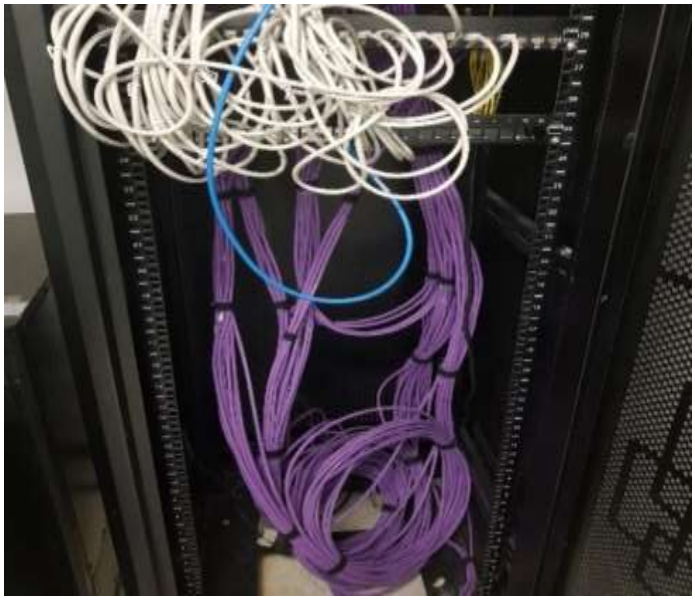
Figura 28. Cielo Raso y cableado de red

Fuente: autor

En la inspección realizada al rack alterno del área de Laboratorio, se encontró que hace falta un organizador para ordenar los *patch cord* que alimentan los

puntos desde el *patch panel* al *Switch*, se debe tener en cuenta que esta es una de las áreas remodeladas.

Figura 29. Rack de datos área de Laboratorio



Fuente: autor

En la revisión a los Racks alternos de (Hospitalización, Urgencias, Vacunación Rita Arango, Fisioterapia Rita Arango, Mantenimiento), estos presentan similitud en cuanto a ubicación y tipo de Rack, por lo tanto se realizarán las observaciones a nivel general, ya que se encuentran en iguales condiciones.

- Estos Racks, son de pared, se encuentran ubicados sobre los pasillos de circulación o en áreas abiertas donde se pueden visualizar por los pacientes y personal ajeno al área de sistemas.

- No se cuenta con la marcación adecuada de los puntos de red.

- Se encontraron switches metidos en el gabinete sobre los cables, sin estar instalados adecuadamente.

- Mucho desorden en el cableado, falta de organizadores de cable.

- Por su ubicación y tamaño dificulta el acceso y trabajo sobre ellos.

- Falta de Mantenimiento periódico, se observa gran cantidad de polvo.

Figura 30. Ubicación de Rack de datos Hospitalización

Fuente. autor

Figura 31. Estado interno de Racks de Pared

Fuente: autor

Finalmente se visitó el Rack de Radiología, donde a pesar de presentar buenas condiciones físicas, se encontraron varias cajas de equipos de cómputo y radiología almacenada allí, lo que no es correcto, por las condiciones descritas anteriormente, ante una posible conflagración.

Figura 32. Rack de Radiología

Fuente: autor

6.4.3 Pruebas de *Pentesting*. Teniendo en cuenta que la ejecución del presente proyecto se están realizando sobre la infraestructura de la red de datos, se realizarán unas pruebas de monitoreo y análisis sobre la red de la entidad, con el fin de identificar posibles vulnerabilidades que puedan afectar la seguridad de la información institucional.

Después de revisar documentación y material de apoyo referente a la materia, se logró identificar las siguientes herramientas basadas en *software* libre, sobre las cuales se realizaron las respectivas pruebas.

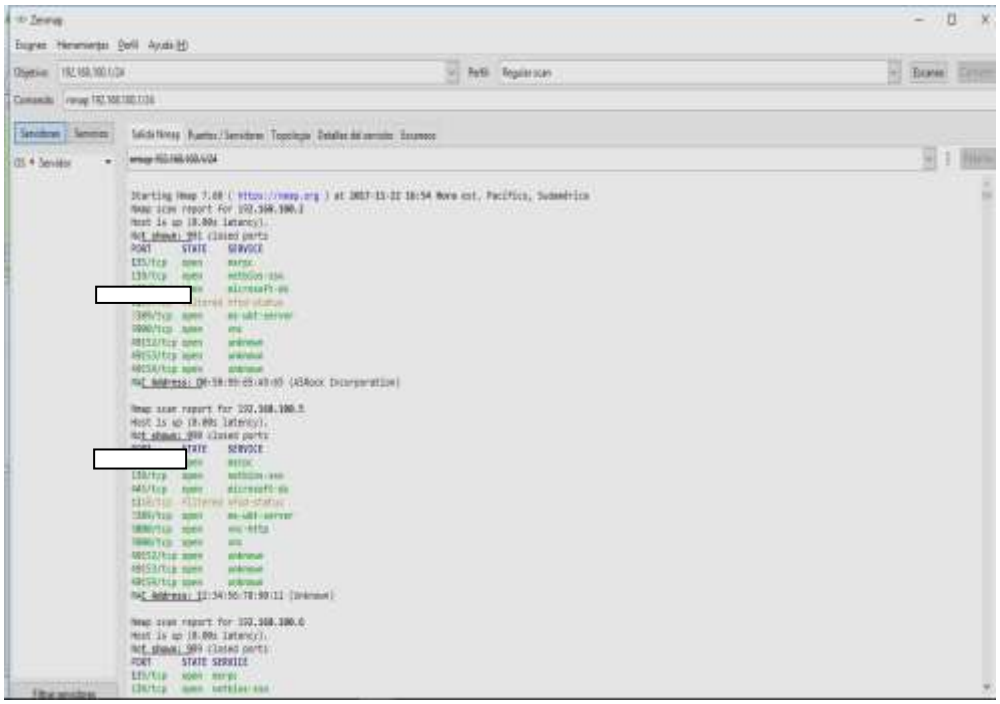
Zenmap: Es la interfaz gráfica del analizador de redes Nmap, está herramienta permite realizar la exploración de cada uno de los hosts que hacen parte de la red monitoreada; allí se puede identificar información relevante como el estado de los puertos, que servicios se ejecutan en ellos, topología de conexión entre los hosts, y otras características que son importantes al momento de realizar una auditoría a la red, vale la pena aclarar que dicha información puede ser utilizada de diferentes formas de acuerdo del perfil de quien la obtenga, ya que si esta es obtenida por el administrador de la red de datos, le permite identificar una serie

de elementos que le pueden causar afectaciones a la infraestructura de la red (preventivo), que al ser asegurados minimizan el riesgo de ataques por explotación de las brechas de seguridad que se puedan presentar; pero si por el contrario esta información es obtenida por personal externo, puede ser utilizada con el fin de atacar y generar daño o robo de información.

Debido a que la información recopilada por la herramienta es estándar, donde se difiere básicamente de acuerdo al *hosts* que información relevante puede mostrar, se realizó una recopilación general y se presentan algunos pantallazos que dan una visión del alcance de la misma.

En la figura 33 se logra visualizar de manera general cada uno de los *hosts* identificados en el escaneo realizado dentro del rango IP de la sede principal, y entrega un resumen de los puertos abiertos en cada uno de ellos.

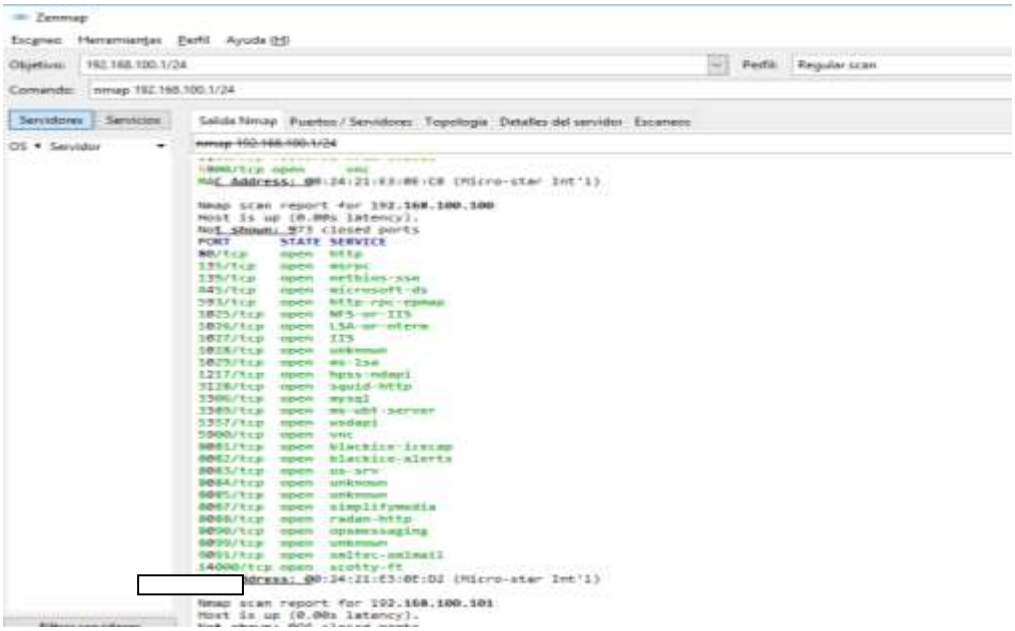
Figura 33. Escaneo Zenmap



Fuente: autor

A continuación se pueden observar los puertos identificados en uno de los servidores de aplicaciones.

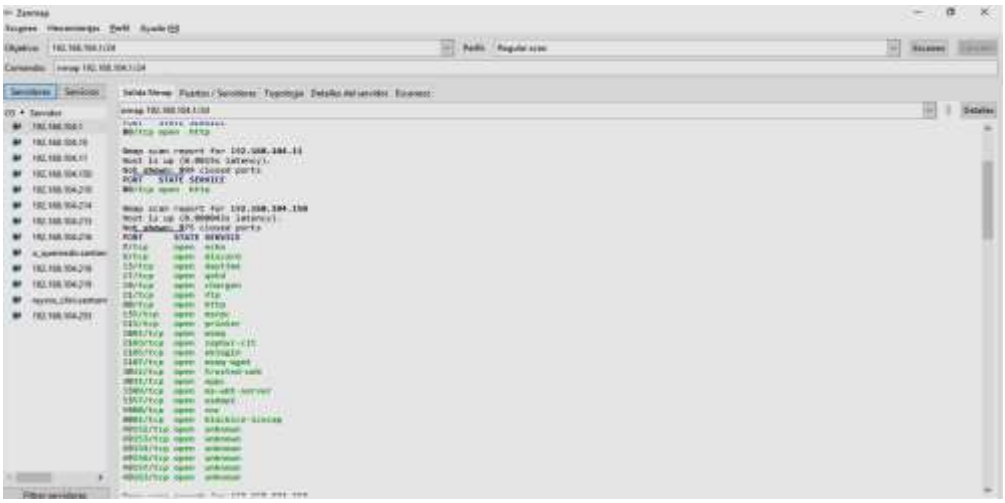
Figura 34. Escaneo Servidor de Aplicaciones



Fuente: autor

En la figura 35 se puede observar información de los *hosts* pertenecientes a una de las subredes, la cual corresponde a una de las sedes alternas (Puesto de salud).

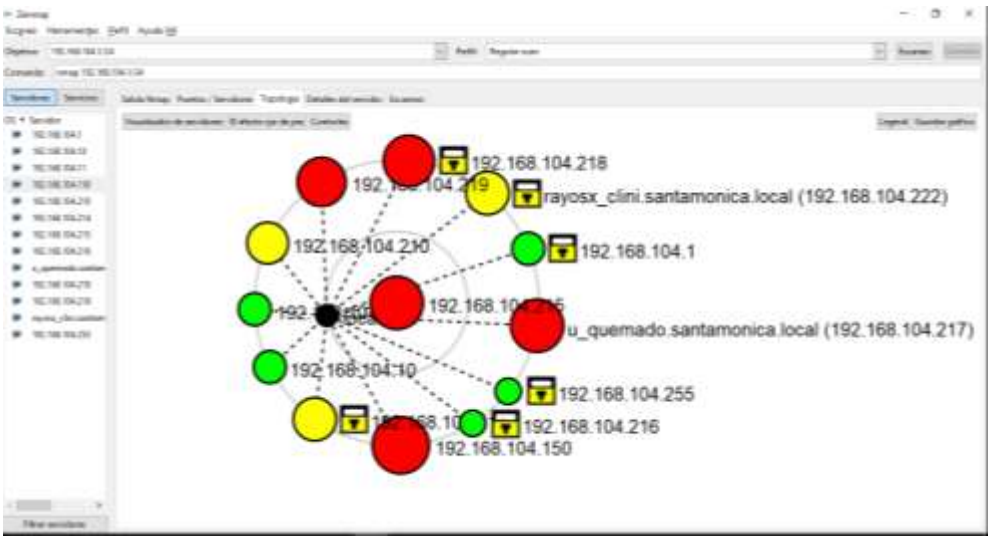
Figura 35.Escaneo Equipo Sede Alterna



Fuente: autor

La figura 36 muestra un gráfico a modo de topología de Red donde se identifican cada uno de los *hosts* interconectados que hacen parte de la red escaneada.

Figura 36. Topología de Red generada por Zenmap



Fuente: autor

Se logra evidenciar, después de ejecutada la herramienta de análisis de red Zenmap, que de una manera rápida se logra ingresar a cada uno de los hosts de la red corporativa, y recopilar la información relevante de los mismos. Sin mucho esfuerzo este identificó y consolidó el estado de los equipos y puertos abiertos, lo cual es información sensible, debido a que esto mal utilizado, y si no se toman las medidas necesarias, para bloquear los puertos que no se requieren, pueden ser puertas abiertas para recibir ataques y vulnerar la seguridad de la red corporativa.

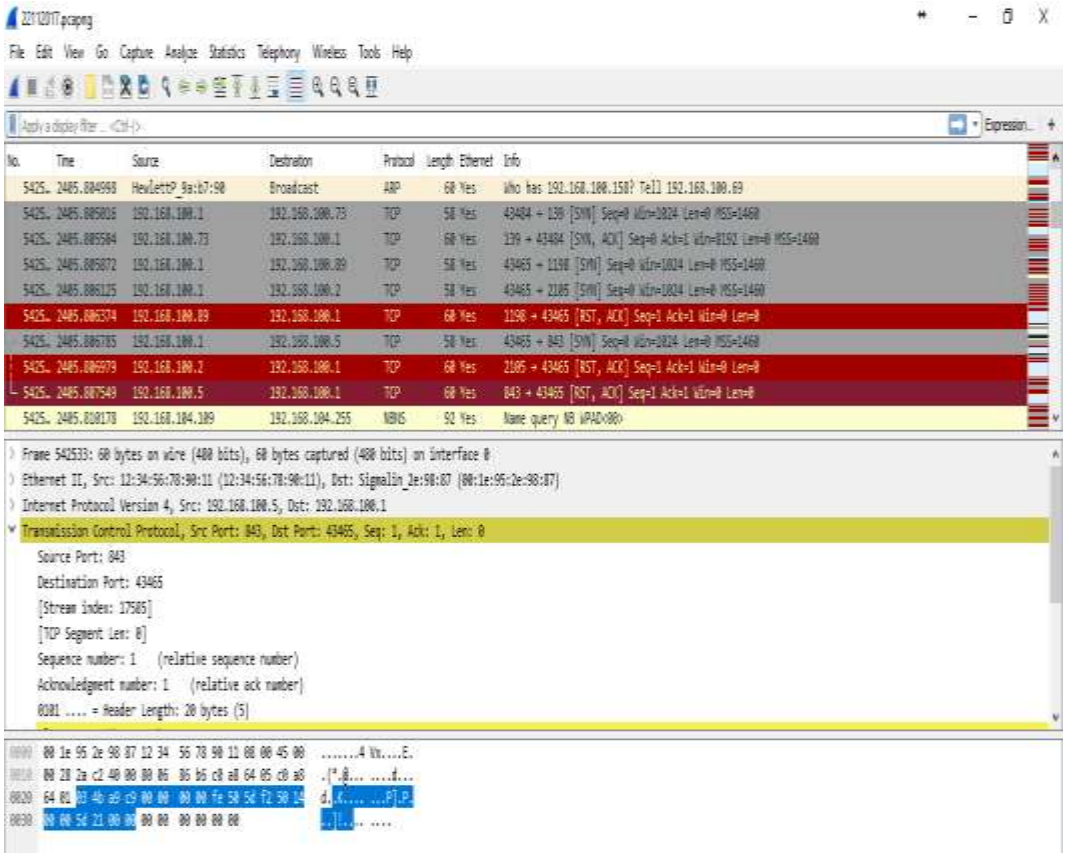
Wireshark: Es una herramienta libre muy interesante, tiene una interfaz gráfica la cual permite analizar el tráfico de red y capturar los paquetes que por allí viajan, seguidamente se puede realizar un análisis de los protocolos utilizados dentro de la comunicación que se presenta entre los diferentes nodos de la red o hacia el exterior.

Esta permite analizar cada uno de los paquetes capturados de manera detallada, y en muchas ocasiones de acuerdo al tipo de protocolo utilizado se puede

visualizar información relevante y sensible como credenciales de acceso a portales.
Aunque esta es una herramienta de mucha ayuda para los administradores de red, ya que les permite analizar el tráfico e identificar problemas de comunicación, que se puedan estar presentando en su red, también mal utilizada por personas inescrupulosas, puede causar daños utilizando esta información de manera inversa; No para corregir errores y cerrar brechas, sino para explotar vulnerabilidades identificadas o robar información.

En la siguiente figura se logra evidenciar el escaneo general que se realiza con la herramienta wireshark, en ella se selecciona por cuales de las tarjetas de red del equipo anfitrión se quiere iniciar el proceso de captura de paquetes, para este caso fue por el adaptador *Ethernet*, e inmediatamente inicia el proceso de escucha y captura de paquetes que viajan por esta red, identificando inicialmente la comunicación entre los *hosts* origen y destino, como los protocolos que utilizan durante este proceso y los puertos de salida y llegada.

Figura 37. Escaneo de Red con Wireshark

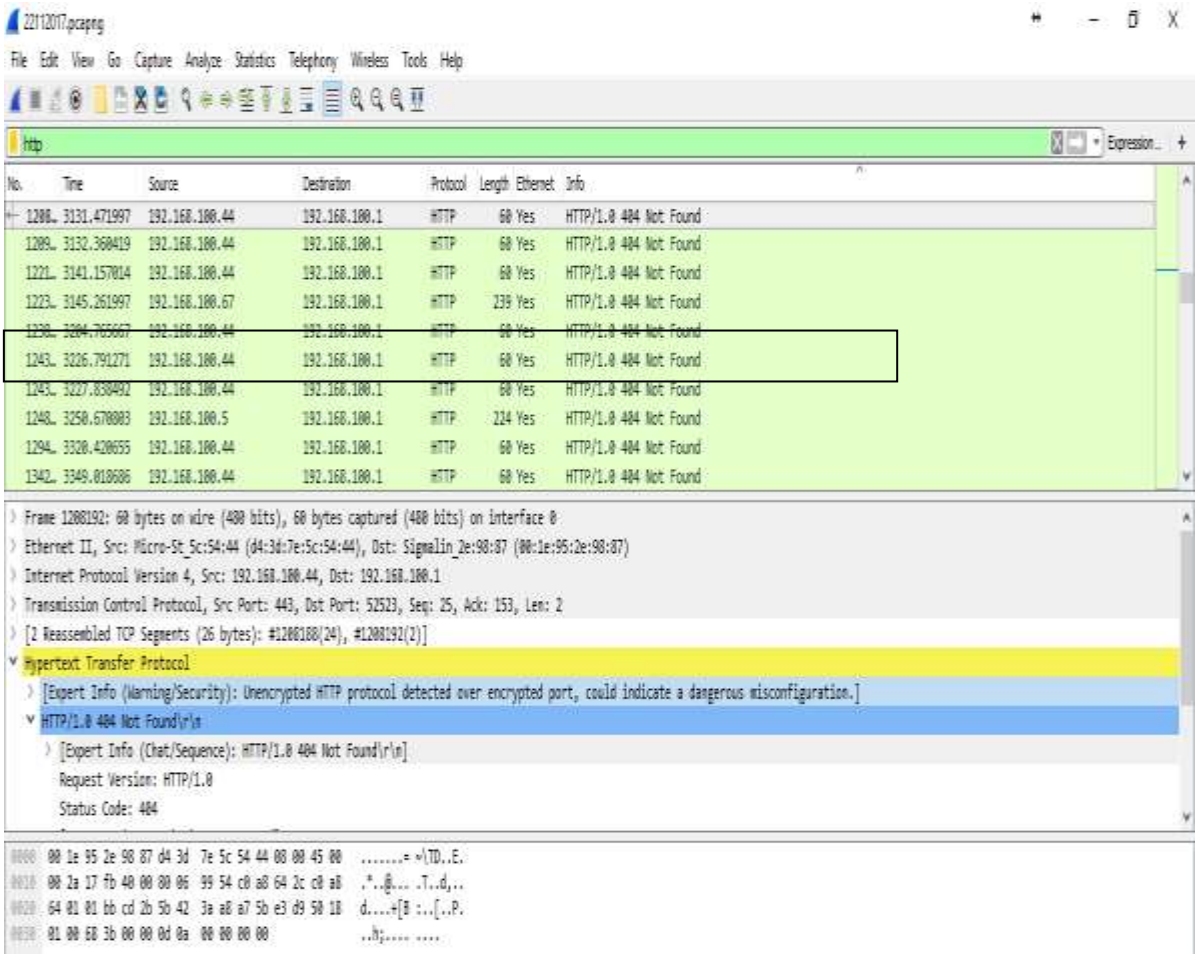


Fuente. autor

En la figura 38 se evidencia, como la herramienta permite realizar una serie de filtros y entre esos por protocolo, para este caso se filtró por el protocolo http, donde trae cada uno de los *hosts* identificados de acuerdo a su dirección IP; que se están comunicando por medio de este protocolo y al seleccionar cada uno de ellos muestra los detalles de los paquetes enviados, lo cual para muchos casos cuando se utiliza un protocolo no seguro o se envía información sin *encriptar* es capturada y visualizada de manera legible, lo que es un riesgo inminente, pues por allí viajan credenciales de acceso a diferentes plataformas, que es información confidencial y por lo tanto debe viajar de tal manera (encriptado), que no sea fácil de descifrar.

También se puede observar en los detalles del paquete capturado alertas de seguridad, de acuerdo al protocolo y los puertos utilizados.

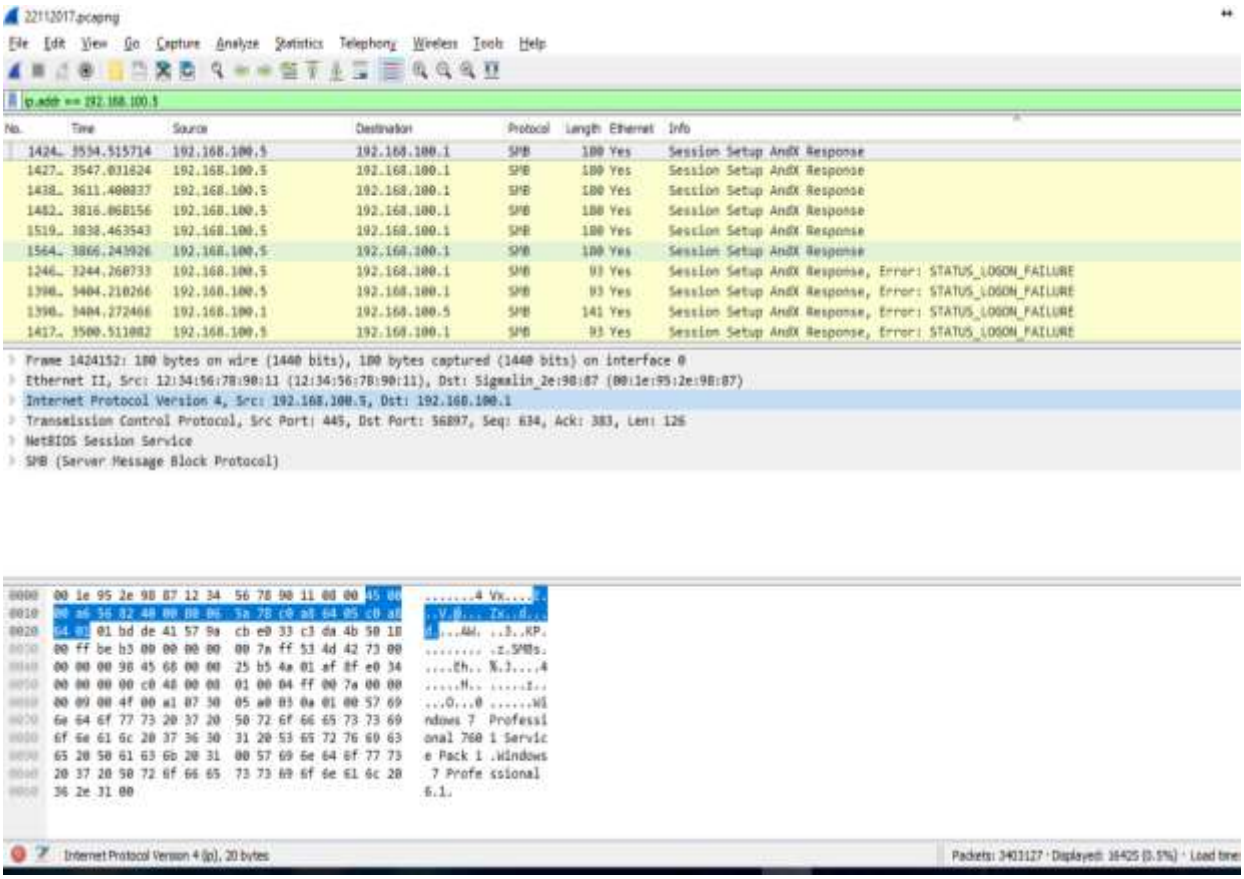
Figura 38. Filtrado por protocolo



Fuente: autor

En la figura 39 se aplicó un filtro por dirección IP, lo que permite realizar seguimiento detallado a un *host* en particular, allí se puede observar en los detalles de los paquetes capturados, información relevante del equipo como el sistema operativo, versión del mismo, protocolos y puertos utilizados

Figura 39. Filtrado por IP



Fuente: autor

Colasoft Capsa: Es una herramienta que permite diagnosticar, monitorear el desempeño de la red, capturar paquetes, análisis de flujo de los datos y sugerir posibles soluciones. Esta aplicación tiene un componente para realizar análisis de seguridad detectando ataques a la red como (Denegación de servicio, ataque ARP, entre otras), permitiendo identificar el origen y objetivo del ataque en tiempo real.

Como se puede apreciar es una excelente herramienta para implementar en la institución, ya que permite tener un monitoreo de la red en tiempo real, e

identificar problemas en general de la misma, la única desventaja es que es un producto comercial; por lo tanto para la verificación realizada se utilizó la versión libre de la misma, la cual tiene una serie de limitaciones entre esas que solo se puede realizar análisis a 10 *hosts*. Teniendo en cuenta que lo que se está realizando es un análisis a la infraestructura de la red de datos en general, se optó por utilizar la herramienta, para detectar vulnerabilidades y fallas que pueden ser extensivas a la red de datos en general.

En la figura 40 se puede apreciar de manera estadistica, el consumo en *bytes* en la linea de tiempo para identificar horas de mayor tràfico, de la misma manera el consumo por *hosts* identificado por su direcciòn IP y por protocolo, los cuales interactuan en el proceso de comunicaciòn y transferencia de informaciòn.

Figura 40. Anàlisis estadistico con Colasoft Capsa free

Fuente: autor

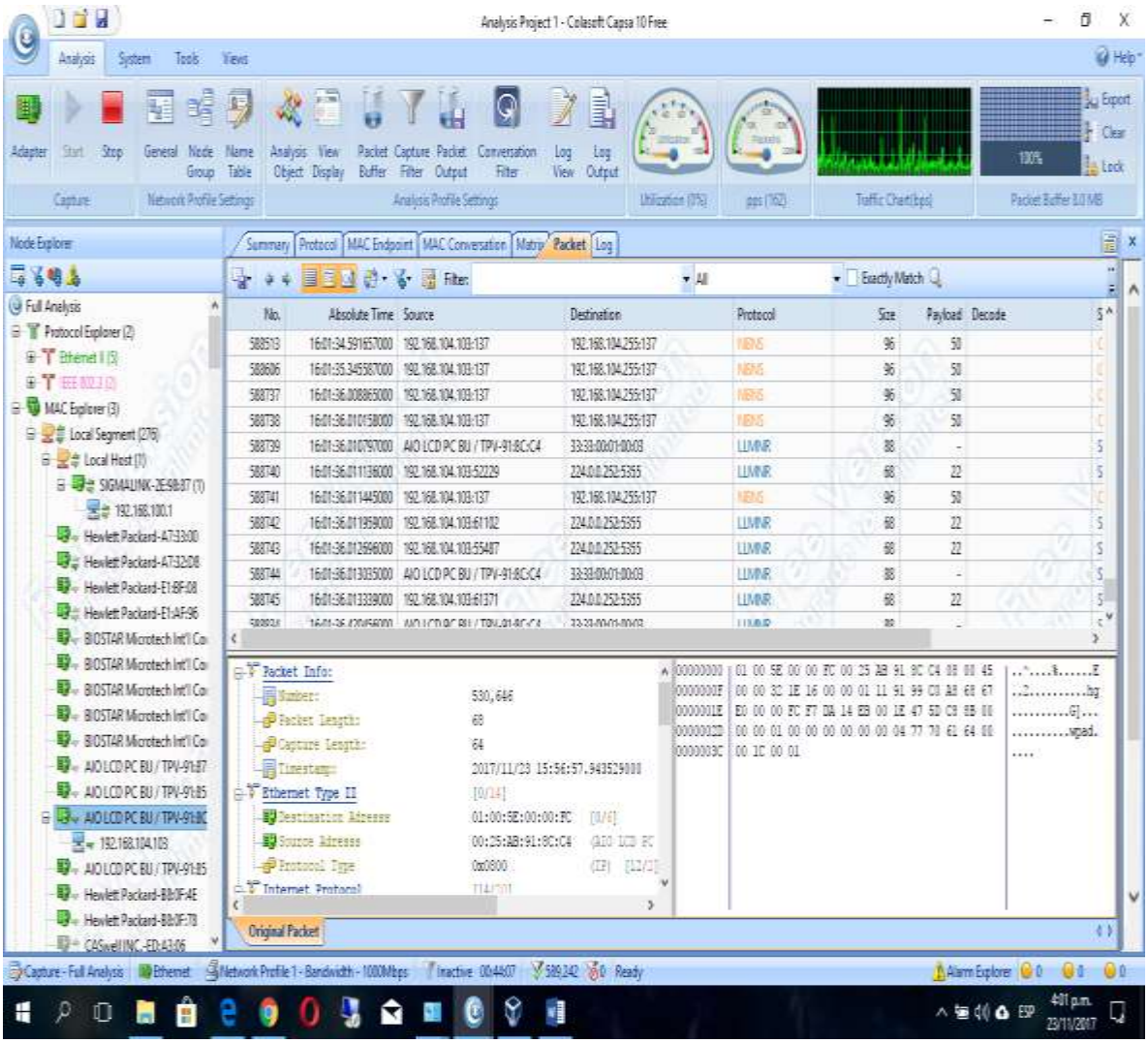
En la figura 41 se puede apreciar los hosts que están interactuando en la transmisión de datos, el protocolo utilizado, el número de paquetes, el tamaño en bytes y los puertos de entrada y salida, información muy importante que pueden marcar tendencias, lo que permite al administrador de seguridad tener herramientas para intervenir sobre estos *host* y verificar actividad maliciosa, que pueda afectar la infraestructura de la red de datos en general, de sus componentes o de la información que se transmite por la misma.

Figura 41. Análisis de Paquetes transmitidos

Fuente. autor

En la figura 42 se puede evidenciar como Colasoft Capsa captura toda la información de los *hosts*, relacionada con las tarjetas de red, como la marca y dirección física (MAC), información sensible, ya que estos son datos importantes, los cuales pueden ser explotados para realizar ataques como (suplantación de identidad, envenenamiento ARP, evasión de filtros MAC, entre otros); por lo tanto de aquí se ve la importancia y relevancia que tiene el poder mantener esta información oculta y que no sea fácilmente visibilizada.

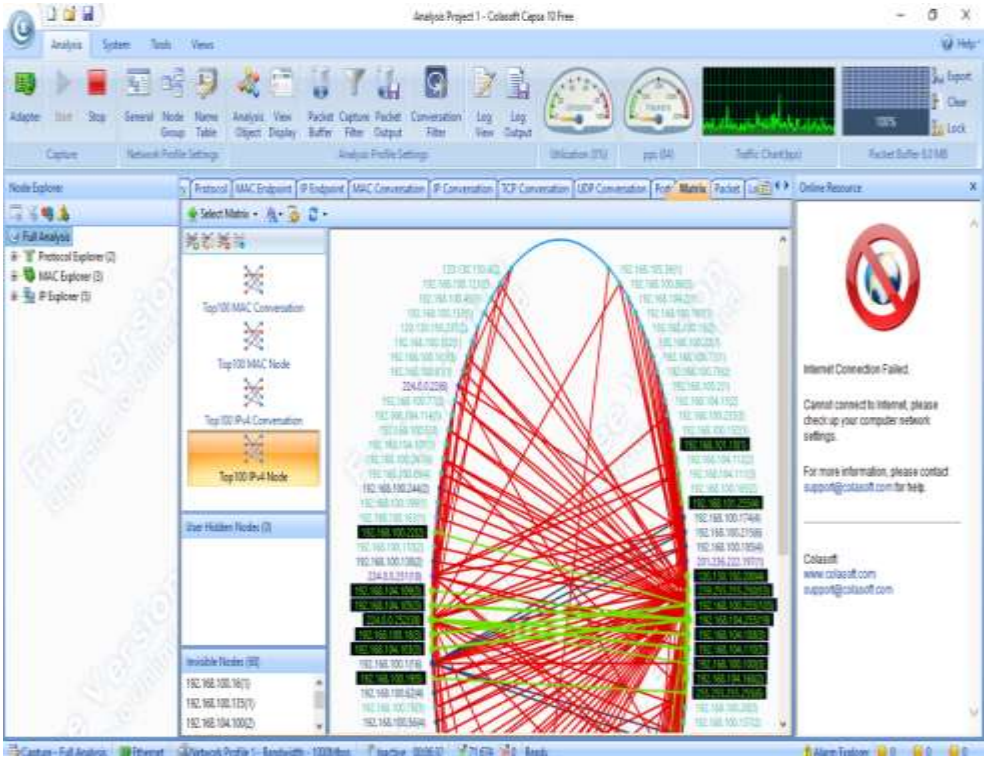
Figura 42. Información MAC Adress



Fuente: autor

En la figura 43 se puede ver de manera gráfica el intercambio de paquetes entre los distintos nodos de la red de datos, los trazos verdes y las direcciones que se encuentran resaltadas, son las que corresponden a los 10 *hosts* que la versión libre de la herramienta permiten analizar.

Figura 43. Comunicación entre hosts de la red de datos



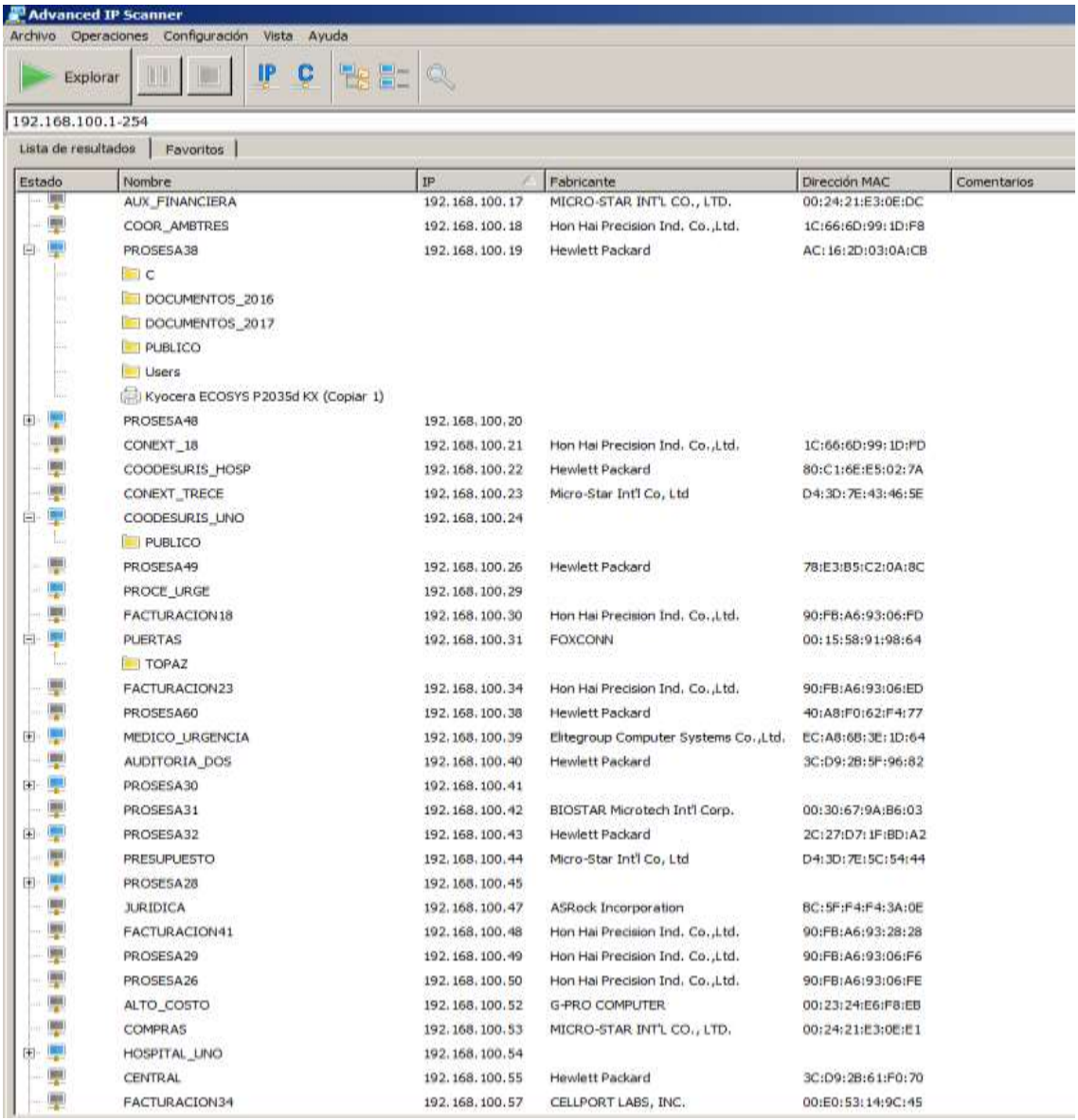
Fuente: autor

Advanced IP Scanner: Es una herramienta gratuita que permite escanear la red de datos, de una manera ágil y sencilla, para lo cual solo requiere indicar el rango IP que se quiere analizar. Esta aplicación permite tener acceso a la información de cada uno de los *host* de la red, otorgando acceso a las carpetas compartidas en la red y a los servidores FTP, adicional a esto presenta otras funcionalidades como (detección de direcciones MAC, Control remoto, Apagado remoto).

Como se puede evidenciar en una herramienta útil y fácil de usar; a los administradores de red o de seguridad de la institución, les brinda información importante sobre todo lo que pueda estar compartido dentro de la red corporativa y ellos puedan desconocer, ya que estas son puertas abiertas para robo de información o para ataques de cualquier tipo, donde lo que se buscan son este tipo de recursos para propagar virus, que al ingresar en uno de los *hosts*, utiliza la red de comunicaciones para difundirse a los demás dispositivos.

En la figura 44 se puede visualizar cada uno de los datos que nos proporciona la herramienta como (Estado del equipo, nombre, IP, Fabricante de Tarjeta de red y la MAC).

Figura 44. Listado de Equipos de la red de datos

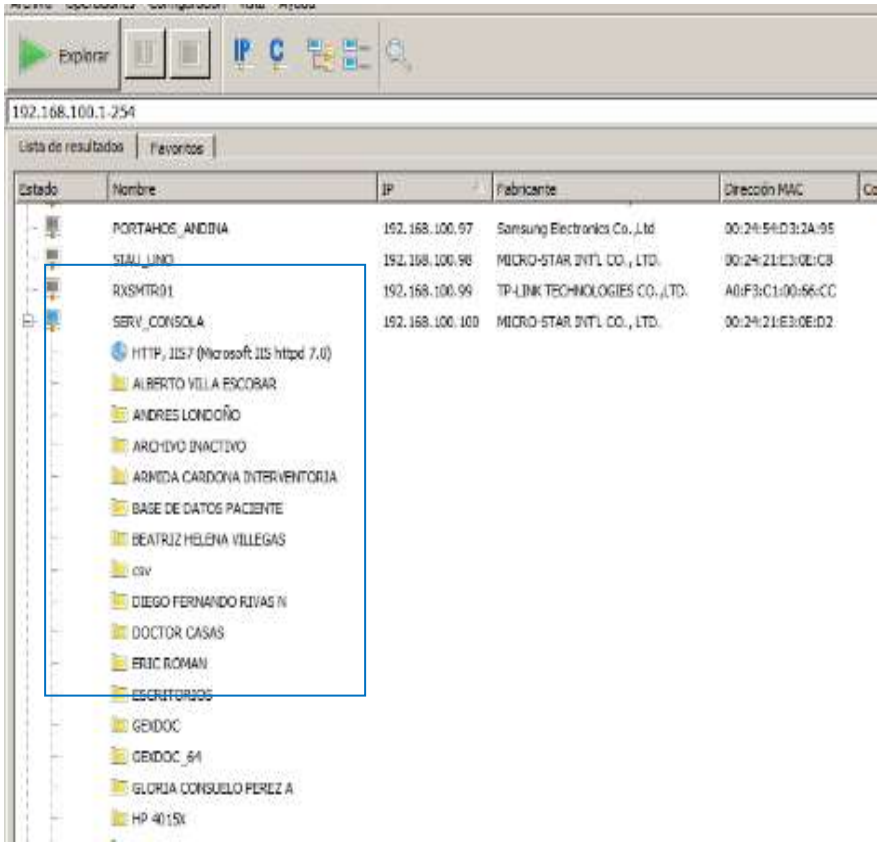


Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
	AUX_FINANCIERA	192.168.100.17	MICRO-STAR INT'L CO., LTD.	00:24:21:E3:0E:DC	
	COOR_AMBTRES	192.168.100.18	Hon Hai Precision Ind. Co.,Ltd.	1C:66:6D:99:1D:F8	
	PROSESA38	192.168.100.19	Hewlett Packard	AC:16:2D:03:0A:CB	
	C				
	DOCUMENTOS_2016				
	DOCUMENTOS_2017				
	PUBLICO				
	Users				
	Kyocera ECOSYS P2035d KX (Copiar 1)				
	PROSESA48	192.168.100.20			
	CONEXT_18	192.168.100.21	Hon Hai Precision Ind. Co.,Ltd.	1C:66:6D:99:1D:FD	
	COODESURIS_HOSP	192.168.100.22	Hewlett Packard	80:C1:6E:E5:02:7A	
	CONEXT_TRECE	192.168.100.23	Micro-Star Int'l Co, Ltd	D4:3D:7E:43:46:5E	
	COODESURIS_UNO	192.168.100.24			
	PUBLICO				
	PROSESA49	192.168.100.26	Hewlett Packard	78:E3:B5:C2:0A:8C	
	PROCE_URGE	192.168.100.29			
	FACTURACION18	192.168.100.30	Hon Hai Precision Ind. Co.,Ltd.	90:FB:A6:93:06:FD	
	PUERTAS	192.168.100.31	FOXCONN	00:15:58:91:98:64	
	TOPAZ				
	FACTURACION23	192.168.100.34	Hon Hai Precision Ind. Co.,Ltd.	90:FB:A6:93:06:ED	
	PROSESA60	192.168.100.38	Hewlett Packard	40:A8:F0:62:F4:77	
	MEDICO_URGENCIA	192.168.100.39	Elitegroup Computer Systems Co.,Ltd.	EC:A8:6B:3E:1D:64	
	AUDITORIA_DOS	192.168.100.40	Hewlett Packard	3C:D9:2B:5F:96:82	
	PROSESA30	192.168.100.41			
	PROSESA31	192.168.100.42	BIOSTAR Microtech Int'l Corp.	00:30:67:9A:B6:03	
	PROSESA32	192.168.100.43	Hewlett Packard	2C:27:D7:1F:BD:A2	
	PRESUPUESTO	192.168.100.44	Micro-Star Int'l Co, Ltd	D4:3D:7E:5C:54:44	
	PROSESA28	192.168.100.45			
	JURIDICA	192.168.100.47	ASRock Incorporation	BC:5F:F4:F4:3A:0E	
	FACTURACION41	192.168.100.48	Hon Hai Precision Ind. Co.,Ltd.	90:FB:A6:93:28:28	
	PROSESA29	192.168.100.49	Hon Hai Precision Ind. Co.,Ltd.	90:FB:A6:93:06:F6	
	PROSESA26	192.168.100.50	Hon Hai Precision Ind. Co.,Ltd.	90:FB:A6:93:06:FE	
	ALTO_COSTO	192.168.100.52	G-PRO COMPUTER	00:23:24:E6:F8:EB	
	COMPRAS	192.168.100.53	MICRO-STAR INT'L CO., LTD.	00:24:21:E3:0E:E1	
	HOSPITAL_UNO	192.168.100.54			
	CENTRAL	192.168.100.55	Hewlett Packard	3C:D9:2B:61:F0:70	
	FACTURACION34	192.168.100.57	CELLPORT LABS, INC.	00:E0:53:14:9C:45	

Fuente: autor

En la figura 45 se visualiza el detalle de los recursos compartidos por cada uno de los equipos conectados a la red.

Figura 45. Recursos compartidos



Fuente: autor

Ingeniería Social: Al culminar con la pruebas de *Pentesting*, y al indagar con los funcionarios de sistemas, acerca de la administración de los CPE que permiten la comunicación de la sede principal, con las distintas sedes ambulatorias, estos manifiestan que la configuración y administración es propia del proveedor de los servicios contratados a nivel local (ISP), que por lo tanto no poseen dicha información.

Como se realizó un recorrido físico por cada una de las sedes y se consolido la información perteneciente a cada uno de los dispositivos, entonces se revisó en internet varios foros donde se hacía referencia a cómo acceder a dichos dispositivos de acuerdo a la marca; donde se marcaba un estándar para acceder

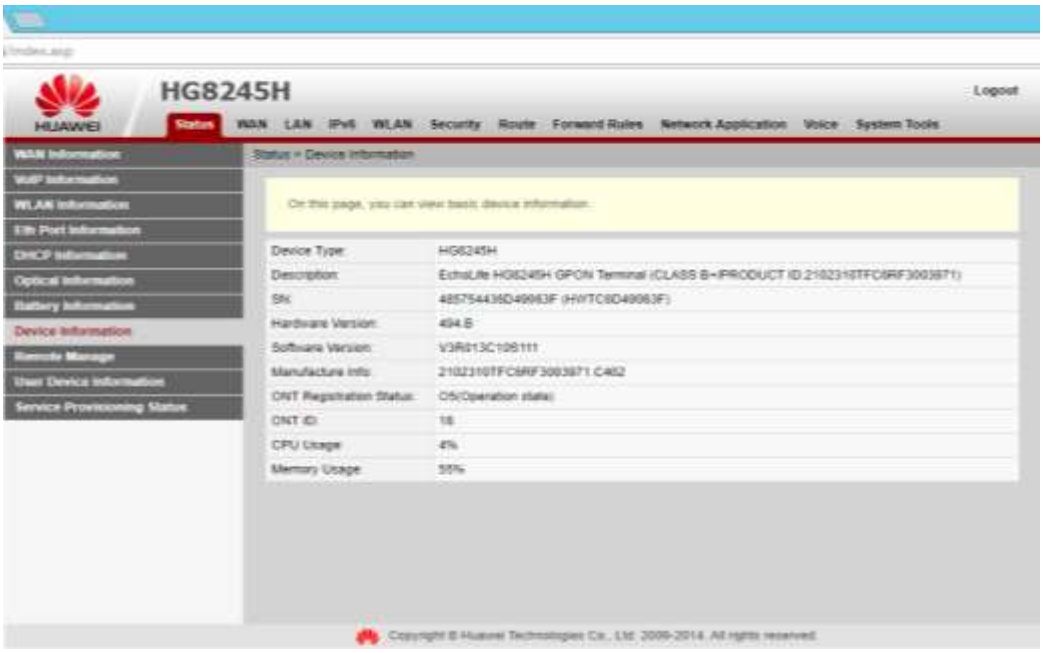
a cada uno de ellos; entonces se tomaron estos datos como referencia y se verificó dicha información tratando de acceder a uno de los dispositivos, de las sedes alternas, que cumplía con las características antes mencionadas.

En la figura 46 se evidencia el acceso a uno de los dispositivos propiedad del ISP, administrados por el proveedor y de los cuales el personal de la Institución no tienen acceso ni administración del mismo.

Figura 46. Acceso a CPE del Proveedor de Internet y transmisión de datos.

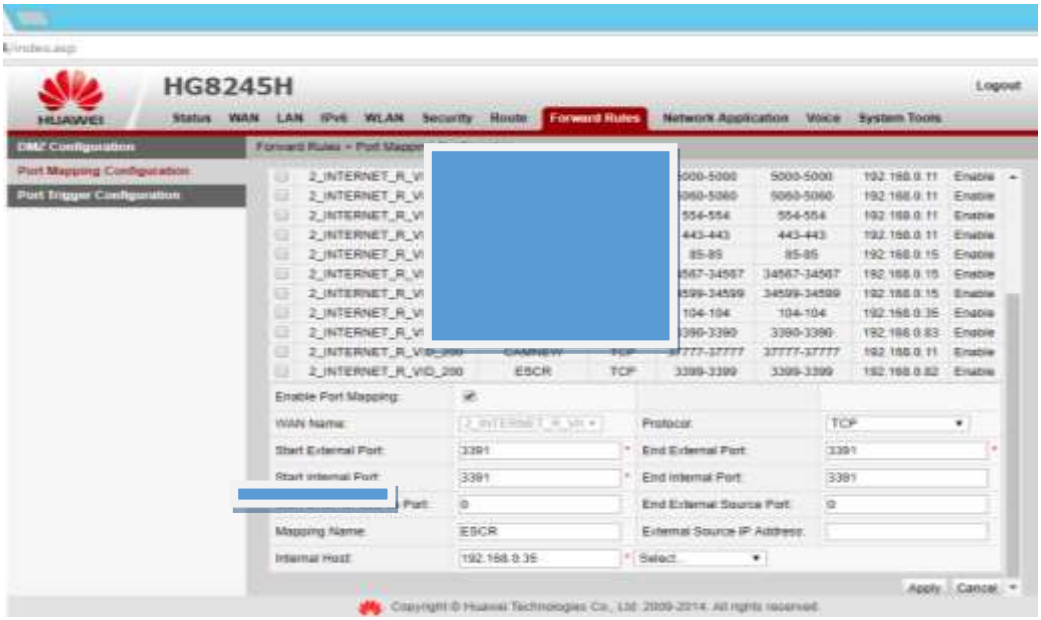
Fuente: autor

Figura 47. Información general del Router



Fuente: autor

Figura 48. Configuración de puertos



Fuente: autor

Como se evidenció en las figuras anteriores, la red de datos, también presenta una evidente brecha de seguridad, debido a que el estándar que manejan para la seguridad de acceso a cada uno de los *routers* del proveedor local (ISP), que presta los servicios de internet y transmisión de datos, ya se encuentra divulgado en internet, y cualquier persona con tan solo buscar dicha información puede acceder a ella de una manera rápida, lo que le permitiría realizar infiltraciones desde el exterior con tan solo poder alcanzar el acceso al *router* que sirve de puente y de esta manera acceder de manera ilegítima a la red local de la institución.

7. HALLAZGOS DE LA INVESTIGACIÓN

Después de la ejecución del Proyecto aplicado a la Entidad E.S.E. Hospital Santa Mónica, el cual se documentó en los ítems anteriores, se procede a mencionar los hallazgos a modo general, que afectan directamente la infraestructura de la red de datos de la Empresa.

- No se cuenta con un Plano de la red de datos de la Entidad, este elemento es de suma importancia; ya que permite tener una identificación de cada uno de los elementos que hacen parte de la infraestructura de la red de datos; y juega un papel vital en el proceso de planeación (ampliación o reestructuración del trazado de la red).

- No se tiene estandarizado la categoría del cableado estructurado, con el que cuenta la red de datos de la Institución, encontrándose áreas conectadas con cableado obsoleto, lo cual genera interferencia que repercute en el funcionamiento general de la red de datos.

- No se cuenta con una Topología de red definida, debido al crecimiento no planeado de la infraestructura de la red de datos, lo que puede desencadenar, en fallas de comunicación o demoras en la transmisión de los datos.

- No se tienen Definidos los estándares para la instalación de los puntos de red en la Entidad, solamente se tienen unos requerimientos mínimos para la instalación de los mismos, dejando esta responsabilidad al libre albedrio del contratista instalador.

- Aunque se cuenta con la Certificación de los puntos de red intervenidos desde el año 2007 a la fecha, no se cuenta con la respectiva certificación de la totalidad de la red de datos; por lo tanto no se tiene un diagnóstico del estado de estos y por ende no se puede garantizar el buen funcionamiento de la red de datos en general.

- No se encuentran actualizados los Dispositivos activos de Red *(Switch, Routers, UTM);* estos dispositivos son instalados con la configuración de fábrica, y no se revisa el *firmware* o actualizaciones vigentes de los mismos, los cuales permiten prevenir fallas de funcionamiento y seguridad.

- No se tiene segmentada la Red de datos en subredes, lo que genera alto tráfico y bajo rendimiento en la red en general, debido a la cantidad de equipos que se encuentran interconectados en la institución.

- No se tiene una identificación apropiada y completa, de cada uno de los elementos que hacen parte de la infraestructura de la red de datos, (puntos de red, dispositivos, Gabinetes, entre otros); lo que dificulta el diagnóstico y reparación de fallas que se presenten en la misma.

- No se tienen implementadas las medidas de seguridad necesarias, para la custodia, monitoreo y acceso a los *Racks* de datos en general, lo que hace que estos sean vulnerables y se puedan violentar con gran facilidad.

- La mayor parte de los *Rack* de datos no cuenta con las condiciones locativas necesarias (pisos, cielos rasos, espacios), sistema de refrigeración (aire acondicionado), y dispositivos de prevención (sensores, alarmas); para garantizar un óptimo funcionamiento de cada uno de los elementos de la infraestructura de la red de datos, y por ende de la red de datos en general.

- Se identificó que gran parte del cableado estructurado de la red de datos que refieren que se ha instalado recientemente, no cumple con la normativa vigente aplicable a este tipo de instalación, ausencia de (*patch panel*, organizadores, marcación, protección); lo que va en contra del adecuado funcionamiento de la red de datos en general.

- Se observó el mal uso de los centros de datos, ya que se encontró material y elementos ajenos al mismo; siendo estos utilizados como bodegas de almacenamiento.

- No se cuenta con la debida organización e instalación de los Dispositivos activos de red, llegando en varios casos a sobreponerse sobre el cableado u otros dispositivos.

- No se evidencia una correcta protección del cableado de red y de las interconexiones en fibra, lo que genera riesgos de daño voluntario o involuntario, por no contar con las medidas de protección necesarias para este tipo de elementos.

- Se evidenció en varios *racks* de datos, la falta de Mantenimiento periódico de los cuartos, gabinetes y de dispositivos de red, lo que puede repercutir en daños o mal funcionamiento, por sobrecalentamiento, o aislamiento de sus componentes.

- Se encontraron algunos dispositivos activos de red obsoletos, lo que genera retardo en el tráfico de datos, lentitud, o mal funcionamiento de la red en general.

- En algunos tramos se encontró que las redes eléctricas, comparten canaleta o ductos con el cableado de datos, lo que provoca ruido, e interferencia, que se ve reflejado en el trabajo inadecuado de la red de datos en general.

- Aunque se tiene documentado el plan de contingencia, este no se encuentra actualizado en su totalidad; lo que hace que ante fallas que se puedan presentar sobre la infraestructura de la red de datos; no brinde las herramientas completas para afrontarlas, debido a que no está aterrizado a la realidad de la Institución.

- Después de realizado el análisis de paquetes y dispositivos interconectados a la red de datos, se logró identificar una serie de puertos que se encuentran activos por defecto, en cada uno de los equipos (TCP 135 – 139 – 445 -1110 – 5800 – 5900 – 3306 – 443, entre otros); estos se encuentran sin ningún tipo de monitoreo, los cuales son altamente sensibles, y pueden ser utilizados como puerta de acceso, para introducir troyanos a la red por alguno de estos equipos, o sufrir ataques como denegación de servicio, suplantación de identidad, robo de información, envenenamiento DNS, captura de paquetes entre otros.

- Se encontró una gran cantidad de recursos compartidos, dentro de cada uno de los equipos conectados a la red de datos de la institución, las cuales son de acceso público y contienen información sensible de la Empresa, no hay ningún tipo de restricción para ingresar a estos, lo que genera un doble riesgo, debido a que dicha información puede ser manipulada (extraída, borrada), por cualquier persona con acceso a la red de datos de la entidad, y también este tipo de recursos son apetecidos por los troyanos para acceder a los equipos y propagarse por toda la red, generando daños y caos en general.

- Aunque se encontró un dispositivo de seguridad UTM, se logró evidenciar que esta subutilizado, ya que solo se tiene implementado para la conexión VPN, y los demás elementos propios del mismo (firewall, control de aplicaciones, IPS, IDS, Filtrado web, entre otros); están inactivos, los cuales brindan herramientas para el endurecimiento de la seguridad informática en la institución.

- Se logró evidenciar que los dispositivos de red instalados y administrados, por el proveedor local de servicios de Internet y Transmisión de datos, son accesibles fácilmente, solo con buscar en internet las características de dichos dispositivos asociados al proveedor; se encuentra el estándar utilizado para las credenciales de acceso, las cuales después de verificadas arrojo el acceso a uno de los dispositivos, de modo que permite manipular la configuración del mismo; lo que atenta contra la seguridad de la red de datos en general, debido a que cualquier persona con tan solo manipular dicha información puede acceder a la red de la institución y generar el caos que quiera.

8. RESULTADOS Y DISCUSIÓN

8.1 PLAN DE MEJORAMIENTO

De acuerdo a los hallazgos realizados durante la ejecución del proyecto aplicado a la ESE Hospital Santa Mónica; se propone el siguiente plan de mejoramiento, con el fin de que la institución lo evalué, y realice los ajustes que crean pertinentes, en aras de fortalecer la seguridad de la infraestructura de la red de datos, y por ende de la seguridad de la información institucional.

Tabla 4. Plan de Mejoramiento Propuesto

ÍTEM	HALLAZGO	SOLUCIÓN PROPUESTA
1	Ausencia de plano de la infraestructura de la red de datos actualizado	Contratar una Consultoría especializada, en redes de datos, para que levante la información necesaria; y de acuerdo a las necesidades de la Institución, realice el montaje del proyecto para la actualización de la infraestructura de la red de datos Institucional. En este proceso debe entregar como parte del proceso de planeación, el plano de la red (aterrizado a la realidad y necesidades futuras de ampliación de la infraestructura física); al igual que debe ir plasmada la topología de red que se debe implementar, y cada uno de los elementos que harán parte del mismo.
2	No se tiene definida una Topología de la red de datos, acorde a las necesidades de la institución.	
3	Ausencia de Patch panel en los racks de datos	Ejecución de Proyecto de Actualización de la Infraestructura de la red de datos, por la Consultoría especializada, contratada para la planeación del Proyecto.

Tabla 4. (Continuación)

ÍTEM	HALLAZGO	SOLUCIÓN PROPUESTA
4	No se tiene estandarizado el cableado estructurado de la red de datos.	Ejecutar el Proyecto basado en la Norma Técnica ANSI/EIA/TIA-568-A, que brinda los lineamientos concernientes, al cableado estructurado para edificios comerciales. "Esta norma específica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante."[20]
5	Cableado de red obsoleto	
6	Falta de protección en algunos Tramos del cableado de red y la fibra óptica que interconecta los gabinetes de datos.	
7	No se tiene certificada la red de datos de la Institución, en su totalidad.	
8	Cableado de red, compartiendo canaletas o ductos con el cableado eléctrico.	
9	No se tiene definido un proceso de estandarización para la instalación de puntos de red e interconexiones en fibra, en la Institución	Definir Estandarización para el proceso de instalación de cableado estructurado de red basado en la Norma Técnica ANSI/EIA/TIA-568-A.
10	No se encuentran identificados y marcados correctamente cada uno de los elementos que hacen parte de la infraestructura de la red de datos (cuartos, gabinetes, punto de red*, patch panel*, entre otros).	Identificación y marcación de la totalidad de elementos que hacen parte de la Infraestructura de la red de datos.

[20] UNIVERSIDAD NACIONAL DE COLOMBIA. "Lineamientos para la elaboración de proyectos de cableado estructurados en la Universidad Nacional". {En línea}. {24 de Noviembre de 2017} disponible en: http://www.unal.edu.co/contratacion/2017/IP_Obra%20_Civil_Tumaco_UN_06102017/Anexo%201.%20Estudios%20tecnicos/Estudios/Informe%20Electrico/LINEAMIENTOS%20PARA%20PROYECTOS%20DE%20CABLEADO.pdf)

Tabla 4. (Continuación)

ÍTEM	HALLAZGO	SOLUCIÓN PROPUESTA
11	Condiciones locativas insuficientes, para el albergue de los diferentes racks de datos (espacios, cielos rasos, pisos falsos, sensores, alarmas, refrigeración).	Reestructuración de los cuartos existentes y reubicación de los racks instalados en espacios abiertos, basados en la norma ANSI/TIA-942-A, "que especifica los requisitos mínimos para infraestructura de telecomunicaciones de centros de datos y salas de computadoras"[21]
12	Controles de seguridad insuficientes, en el acceso y monitoreo de cada uno de los *Racks* de datos y de los elementos que los componen.	Implementar circuito cerrado de televisión para el monitoreo de los centros de datos. Implementar control de acceso, con el fin de garantizar que el personal que ingrese a los mismos sea autorizado, y donde se registre la actividad ejecutada, durante el ingreso.
13	No se cuenta con segmentación de la red de datos de la Institución	Proceso que se debe incluir dentro del proyecto de actualización de la infraestructura de la red de datos.
14	Se evidenciaron, varios dispositivos activos de red, obsoletos	Reponer los dispositivos activos de red que se encuentran obsoletos, y no son administrables.
15	No se ejecutan procesos de actualización periódica, de *firmware* de los dispositivos activos de red.	Implementar Política para la actualización periódica de los Dispositivos activos de red.
16	Mal uso de los cuartos que albergan los Racks de Datos, utilizados como bodegas.	Implementar Políticas del uso adecuado de los centros de datos, y restricción de acceso a personal ajeno al área encargada de los mismos.

[21] WIKIPEDIA. "TIA-942" {En línea}. {24 de Noviembre de 2017} disponible en: https://en.wikipedia.org/wiki/TIA-942

Tabla 4. (Continuación)

ÍTEM	HALLAZGO	SOLUCIÓN PROPUESTA
17	Dispositivos activos de red, no se encuentran instalados adecuadamente	Proceso que se debe incluir dentro del proyecto de actualización de la infraestructura de la red de datos.
18	Falta de un adecuado mantenimiento a los gabinetes y dispositivos de red.	Ejecutar a cabalidad el cronograma de mantenimiento anual.
19	Plan de contingencia desactualizado	Actualizar el Documento establecido, como Plan de Contingencia, aterrizado a la realidad de la Institución.
20	Ausencia de Políticas de Seguridad, enfocadas a la infraestructura de la red de datos, con énfasis en la seguridad informática	Creación de las políticas de Seguridad, que vayan encaminadas a la protección de la Infraestructura de la red de datos.
21	Recursos de red compartidos, con acceso público, con contenido sensible de la empresa.	Revisión de todos los recursos compartidos, y restricción de los mismos, de tal manera que el acceso solo sea permitido al personal que lo requiera.
22	Puertos en los equipos de red abiertos, sin ningún tipo de monitoreo o restricción.	Cerrar todos los puertos que se encuentren habilitados en los dispositivos de red, que no sean requeridos para el funcionamiento normal de la red de datos en general.
23	No se cuenta con sistemas de Prevención y detección de Intrusiones (IPS, IDS).	Analizar si el dispositivo UTM Fortinet que tienen subutilizado, soporta la cantidad de equipos de la Institución, o sino implementar un modelo que soporte la infraestructura donde se habiliten cada uno de los servicios y funcionalidades que brindan estos como: Firewall, Detección y Prevención de Intrusiones, Control de aplicaciones, Filtrado Web, entre otros.
24	Dispositivo UTM de seguridad perimetral, subutilizado, solo para el control y acceso a la red por medio de VPN, demás módulos de seguridad inhabilitados (Firewall, Filtrado Web, entre otros).	

Tabla 4. (Continuación)

ÍTEM	HALLAZGO	SOLUCIÓN PROPUESTA
25	Dispositivos de red, administrados y configurados por el Proveedor local de los servicios de Internet y Transmisión de datos, con credenciales de acceso publicadas en internet.	Solicitar al Proveedor local de los servicios de internet y transmisión de datos la revisión de las políticas para la creación de credenciales de acceso a sus dispositivos de red, en procura de velar porque dicha información no se haga pública.

Fuente: autor

8.2 IMPACTO

Teniendo en cuenta; que la institución tiene dentro de su plan de desarrollo, estipulado la ejecución del proyecto referente a la actualización de la Infraestructura de la red de datos sustentado en lo obsoleto de las redes; con el desarrollo del proyecto aplicado se logró concientizar al área de Tecnología en Cabeza de la Coordinadora Sandra Echeverry, de la importancia de la ejecución de este, pero no enmarcado solo en cambiar los elementos físicos, por lo obsoleto de los mismos, sino sustentado bajo la luz de la seguridad informática, de cómo el estado actual de los elementos físicos y configuraciones inapropiadas de los dispositivos activos de red, atentan contra la seguridad de la información institucional, y de qué manera deben ampliar el espectro para soportar el proyecto que presenten a la alta dirección; sustentado en una inversión que permitirá proteger el activo más importante de la Institución como lo es los datos y la información, y no como un gasto operacional. Esto debido a que por el tamaño de la Institución, el estado actual de la infraestructura y partiendo de la premisa que el mismo se ejecutará, con el fin de atacar todos los frentes que pueden afectar la infraestructura de la red de datos, este tiene un alto costo económico, un factor que en las instituciones de salud del sector público tiene una mayor complejidad por los presupuestos aprobados, en especial por el rubro de inversión.

Por lo tanto; los objetivos del proyecto encaminados a la toma de conciencia por parte de la institución se cumplieron, ya que el área de tecnología, quedo alerta por los riesgos a los que están expuestos, y quedaron muy dispuestos, de ejecutar las tareas y acciones que se encuentren al alcance de ellos (con los recursos tecnológicos actuales), para empezar a cerrar las brechas de seguridad

y minimizar los riesgos o impactos a los que se puedan ver abocados por el estado actual de la infraestructura de la red de datos.

8.3 RESULTADOS OBTENIDOS

El resultado esperado, estaba enfocado a la toma de conciencia por parte de la institución; en beneficio de la preservación de la seguridad de la información, lo cual se logró con la ejecución del proyecto, ya que se recibió de muy buena forma el desarrollo del mismo, y se brindaron las herramientas necesarias para llevar el mismo a feliz término.

9. CONCLUSIONES

- Se logró evidenciar una serie de vulnerabilidades y debilidades en la Infraestructura de la red de datos, que aunque el personal del área de tecnología tiene identificadas algunas de ellas; las cuales se dilucidaron en la etapa inicial, en la ejecución de la Entrevista, no tenían claro, el impacto o la magnitud del riesgo a el que están expuestos.

- Aunque el área de Tecnología de la información, cuenta con un personal comprometido en cabeza de la Coordinadora, se evidencio gran desconocimiento, en materia de seguridad informática; y que esta no solo pasa con tener configurado un antivirus.

- Se logró demostrar al área de Tecnología de la Empresa que hay una serie de herramientas de *Software* Libre, disponibles que permiten implementar medidas preventivas a través del monitoreo y detección de vulnerabilidades, sin hacer grandes inversiones económicas.

- Con la entrega al área de Tecnología de la Empresa de las recomendaciones y el plan de mejora propuesto, que salió del presente proyecto, se da un insumo importante para que sea analizado y puesto en marcha en aras de preservar la Seguridad Informática Institucional.

- Las limitaciones que se dan en la Empresa; para la implementación de proyectos de impacto tecnológico, son de orden presupuestal; debido al tipo de Institución, donde en la actualidad el Sector Salud en el país se encuentra en crisis.

- Con la ejecución del proyecto aplicado, se generó conciencia en el personal Técnico del área de Tecnología de la Información, sobre la importancia que tiene mantener en buen estado la Infraestructura de redes de datos; y que esta solamente no se compone de elementos físicos (*Switch, Router*, Cableado); sino de otros elementos lógicos (Configuración, Políticas), que a la postre son los más importantes bajo la óptica de la Seguridad Informática; ya que son los encargados de minimizar los riesgos e impactos a los cuales se encuentre expuesto la red de datos Institucional.

- La Institución ha sido receptiva y colaboradora con la ejecución del proyecto, debido a que son conscientes que el uso de buenas prácticas se traduce en mayor productividad y tranquilidad en cada una de sus áreas, desde la Oficina de Tecnología, hasta la Alta Gerencia.

10. RECOMENDACIONES

Las recomendaciones específicas se realizaron en el plan de mejoramiento, basadas en los hallazgos realizados durante la ejecución del proyecto aplicado, a la Infraestructura de la red de datos de la ESE Hospital Santa Mónica; sin embargo a continuación se enumeraran otras de forma general.

- Solicitar a la Gerencia de la Institución la capacitación continua del personal del área de tecnología en temática relacionada con la seguridad informática, con el fin de implementar las mejores prácticas al interior de la institución.

- Implementar las políticas de Seguridad Institucionales, en aras de minimizar los riesgos e impactos a los que se pueda ver abocada la Institución por brechas de seguridad, no identificadas.

- Consultar los manuales de Hardening (Endurecimiento), de cada uno de los dispositivos activos de red, donde se dan las pautas, de las mejores prácticas, para la configuración de los mismos.

- Elaborar el proyecto de actualización de la Infraestructura de la red de datos, sustentado bajo la luz de la seguridad Informática, y apoyado en las diferentes Normas Técnicas que definen los lineamientos para este tipo de Proyectos.

- Revisar, complementar y ejecutar el plan de mejoramiento propuesto, en beneficio de la seguridad Informática Institucional.

- Concientizar a la totalidad del personal de la Empresa, en la importancia del manejo seguro de la información, basado en los lineamientos de la seguridad informática.

- Explorar otros tipos de financiamiento de los proyectos de Tecnología, buscando el apoyo del Gobierno Central; a través de la presentación de estos, al banco de proyectos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

- Minimizar los riesgos asociados al *Sniffing,* para evitar este tipo de aplicaciones en la red de la Empresa, se debe partir por implementar controles desde el área de tecnología de la información; iniciando desde los más básicos, hasta los más específicos; para esto se enumeran a continuación algunos a tener en cuenta.

- Limitar y denegar la conexión de equipos de cómputo ajenos a la institución a la red de Corporativa.

- Limitar la ejecución de cualquier tipo de instalador de aplicaciones, en los equipos de la Institución a personal ajeno al área de Tecnología de la Información.

- Explorar e implementar herramientas basadas en Software Libre, para el monitoreo y Detección de Intrusos.

- Realizar un mantenimiento periódico de los equipos de la Empresa a nivel de *Software,* eliminando todo aquello que no deba estar instalado, en cada uno de los equipos de cómputo.

- Actualizar periódicamente, sistemas operativos y *firmware* de los Dispositivos Activos de Red (*Switch, Router*, Servidores, PCs).

- Mantener actualizadas las soluciones de seguridad implementadas al interior de la Institución.

Aquí se dejan algunas recomendaciones que se pueden implementar a nivel general, pero sin dejar de un lado, la actualización permanente de cada uno de los integrantes del área de tecnología en temas relacionados con Seguridad Informática, ya que es una temática con un alto grado de cambio constante.

11. DIVULGACIÓN

Con el fin de dar a conocer el Proyecto aplicado a la ESE Hospital Santa Mónica se realizó Informe que contiene, los apartes más relevantes del presente documento, y se socializo con los integrantes del área de tecnología de la Información; más sin embargo la Coordinación solicito tener una copia del Proyecto completo, como un insumo para gestionar ante la Gerencia la ejecución de los proyectos que tiene aplazado en materia Tecnológica en especial en la Infraestructura de la red de datos.

BIBLIOGRAFÍA

ACTUALISALUD. “Resolución 839 de 2017”. {En línea}. {consultado el 07 de Noviembre de 2017} disponible en: (http://www.actualisalud.com/index.php/ usuarios-registrados-online/379-resolucion-839-de-2017)

ANÓNIMO, “Definición de Modelo OSI”. {En línea}. {05 de Noviembre de 2017} disponible en: (https://sites.google.com/site/stigestionydesarrollo/ recuperacion/ desarrollo-1/recuperacion-provisional/5---describir-el-modelo-osi-definicion-utilidad-y-niveles

BATANERO, Cristian Camilo y BELTRÁN, Diego Alejandro. Diseño de un plan de mejoramiento del sistema de seguridad físico y lógico de acuerdo con modelos de gestión de la infraestructura de redes aplicable a una Institución Educativa. Trabajo de grado Ingeniero en Telecomunicaciones. Bogotá D.C.: Universidad Militar Nueva Granada. 2012, {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: http://repository.unimilitar.edu.co/ bitstream/10654/7211/2/JaimeBataneroCristianCamilo2012.pdf

BUSTA, María José. “Principios Básicos de Seguridad TI”. {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (https://www. hostname.cl/blog/principios-basicos-de-seguridad-ti)

DE MAYA, David. “Hardening de nuestro Centro de Datos”. {En línea}. {05 de Noviembre de 2017} disponible en: (https://hardsoftsecurity.es/ hardening DeNuestroCentroDeDatosv2.pdf)

DELTA. “Ley de Delitos Informáticos en Colombia”. {En línea}. { consultado el 07 de Noviembre de 2017} disponible en: (http://www.deltaasesores.com/articulos/ autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia)

1&1 DIGITAL GUIDE. . “MPLS: estándar de transporte de datos en redes”. {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (https://www.1and1.es/digitalguide/servidores/know-how/mpls-que-es-el-multiprotocol-label-switching/

ENTER.CO S.A.S. El hacking ético y su importancia para las empresas [En línea], {consultado el 05 de Noviembre de 2017} disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario>

GALINDO, José Fernando. “Dispositivos Activos de Red”. {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (https:// senaintro.

blackboard.com/bbcswebdav/institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_disp_activos/utilidades/descargable.pdf

GÓMEZ, Álvaro. “Enciclopedia de la Seguridad Informática. 2ª edición”. {En línea}. { consultado el 17 de Febrero de 2018} disponible en: (https://books.google.es/books?hl=es&lr=&id=Bq8-DwAAQBAJ&oi=fnd&pg=PT2&dq=define+seguridad+informatica&ots=dwlbZj3gaJ&sig=bIOP5Y7p4Cvd6-ZavJfXfm4rFkw#v=onepage&q=define%20seguridad%20informatica&f=false).

GUZMÁN, Alexander y TABORDA, Carlos Alberto. Diseño de un sistema de gestión de la seguridad informática – SGSI -, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoría. Trabajo de grado Especialista en Seguridad Informática. Bogotá D.C.: Universidad Nacional Abierta y a Distancia. 2015, {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3448/1/1030548291.pdf

ISOTools Excellence. “ISO 27001: ¿Qué significa la Seguridad de la Información?”. {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion).

MAYOL R, Modelo para la auditoría de la seguridad Informática en la red de datos de la Universidad de los Andes, Venezuela, {En línea}. {consultado el 05 de Noviembre de 2017} disponible en:http://tesis.ula.ve/postgrado/tde_busca/arquivo.php?codArquivo=114

MICROSOFT. “Definición de las siete capas del modelo OSI y explicación de las funciones”. {En línea}. {05 de Noviembre de 2017} disponible en: https://support.microsoft.com/es-es/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

MINISTERIO DE SALUD. “Resolución número 1995 de 1999”. {En línea}. {07 de Noviembre de 2017} disponible en: (https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Lineamientos de política para ciberseguridad y ciberdefensa. {En línea}. {consultado el 07 de Noviembre de 2017} disponible en: (https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf)

PERAFÁN, John Jairo y CAICEDO, Mildred. Análisis de riesgos de la seguridad de la información para la institución universitaria Colegio Mayor del Cauca. Tesis de grado Especialista en Seguridad Informática. Popayán: Universidad Nacional Abierta y a Distancia. 2014,{En línea}. {consultado el 05 de Noviembre de 2017} disponible en:http://repository.unad.edu.co/handle/10596/2655

PÉREZ, Julián y MERINO María. “Definición de Red de Datos”. {En línea}. { consultado el 05 de Noviembre de 2017} disponible en: (https://definicion.de/red-de-datos/).

RAMÍREZ, Jorge Enrique. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander. Trabajo de grado Especialista en Seguridad Informática. Pamplona: Universidad Nacional Abierta y a Distancia. 2015. {En línea}. {consultado el 05 de Noviembre de 2017} disponible en:¨ http://repository.unad.edu.co/bitstream/ 10596/3415/1/88030934.pdf

UNIVERSIDAD NACIONAL DE COLOMBIA. “Lineamientos para la elaboración de proyectos de cableado estructurados en la Universidad Nacional”. {En línea}. {24 de Noviembre de 2017} disponible en: http://www.unal.edu.co/contratacion/2017/IP_Obra%20_Civil_Tumaco_UN_06102017/Anexo%201.%20Estudios%20tecnicos/Estudios/Informe%20Electrico/LINEAMIENTOS%20PARA%20PROYECTOS%20DE%20CABLEADO.pdf)

VIALFA, Carlos. “Tipos de Redes”. {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: (http://es.ccm.net/contents/257-tipos-de-redes).

WIKIPEDIA. “TIA-942” {En línea}. {24 de Noviembre de 2017} disponible en:https://en.wikipedia.org/wiki/TIA-942

ANEXOS

Anexo A. APROBACIÓN DESARROLLO PROYECTO APLICADO EN LA ESE HOSPITAL SANTA MÓNICA POR PARTE DEL PERSONAL DIRECTIVO

Dosquebradas 27 de Abril de 2015

Doctor:
JAVIER ALEJANDRO GAVIRIA M.
Gerente
ESE Hospital Santa Mónica
Dosquebradas

Referencia: SOLICITUD APROBACIÓN, DESARROLLO PROYECTO APLICADO EN LA ESE HOSPITAL SANTA MÔNICA EN EL AREA DE SEGURIDAD INFORMÁTICA.

Reciba un cordial Saludo.

Me remito a usted muy respetuosamente con el fin de solicitarle, me sea autorizado desarrollar mi proyecto de grado aplicado en la ESE Hospital Santa Mónica, en el área de Seguridad Informática, como requisito de graduación para la especialización que actualmente curso de Seguridad Informática en la Universidad Nacional Abierta a Distancia (UNAD).

Agradezco de antemano la atención y colaboración brindada.

Atentamente,

JONATHAN ARISMENDI RAMÍREZ
C.C. 18.520.719 de Dosquebradas
Ingeniero de Sistemas
ESE Hospital Santa Mónica

Visto Bueno
SANDRA C. ECHEVERRY
Coordinadora Sistemas de Información
ESE Hospital Santa Mónica

Visto Bueno
JAVIER ALEJANDRO GAVIRIA
GERENTE
ESE Hospital Santa Mónica

Anexo B. RESUMÉN ANÁLITICO ESPECIALIZADO (RAE)

1. Información General	
Título:	Análisis de riesgos y diagnóstico de la seguridad de la información de la ESE Hospital Santa Mónica, bajo los parámetros de la seguridad informática.
Autor:	Jonathan Arismendi Ramírez
Director:	Esp. Seguridad Informática Julio Vargas
Fuente Bibliográfica	Para el presente proyecto se referencian 22 fuentes Bibliográficas a continuación se mencionan algunas de ellas: • GÓMEZ, Álvaro. "Enciclopedia de la Seguridad Informática. 2ª edición". {En línea}. { consultado el 17 de Febrero de 2018} disponible en: (https://books.google.es/books?hl=es&lr=&id=Bq8-DwAAQBAJ&oi=fnd&pg=PT2&dq=define+seguridad+informatica&ots=dwlbZj3gaJ&sig=bIOP5Y7p4Cvd6-ZavJfXfm4rFkw#v=onepage&q=define%20seguridad%20informatica&f=false). • MAYOL R, Modelo para la auditoría de la seguridad Informática en la red de datos de la Universidad de los Andes, Venezuela, {En línea}. {consultado el 05 de Noviembre de 2017} disponible en: http://tesis.ula.ve/postgrado/tde_busca/arquivo.php?codArquivo=114 • PERAFÁN, John Jairo y CAICEDO, Mildred. Análisis de riesgos de la seguridad de la información para la institución universitaria Colegio Mayor del Cauca. Tesis de grado Especialista en Seguridad Informática. Popayán: Universidad Nacional Abierta y a Distancia. 2014,{En línea}. {consultado el 05 de Noviembre de 2017} disponible en:http://repository.unad.edu.co/handle/10596/2655 • RAMÍREZ, Jorge Enrique. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander. Trabajo de grado Especialista en Seguridad Informática. Pamplona: Universidad Nacional Abierta y a Distancia. 2015. {En línea}. {consultado el 05 de Noviembre de 2017} disponible en:¨ http://repository.unad.edu.co/bitstream/10596/3415/1/88030934.pdf • UNIVERSIDAD NACIONAL DE COLOMBIA. "Lineamientos para la elaboración de proyectos de cableado estructurados en la Universidad Nacional". {En línea}. {24 de Noviembre de 2017} disponible en: http://www.unal.edu.co/contratacion/2017/IP_Obra%20_Civil_Tumaco_UN_06102017/Anexo%201.%20Estudios%20tecnicos/Estudios/Informe%20Electrico/LINEAMIENTOS%20PARA%20PROYECTOS%20DE%20CABLEADO.pdf)

Año:	2017
Resumen:	La ejecución del proyecto Aplicado, se desarrolla sobre una Institución de Salud de Carácter público, de segundo nivel de complejidad; la cual se encuentra ubicada en el municipio de Dosquebradas, Departamento de Risaralda. Por ser una institución de Salud maneja información altamente sensible, como lo es todo el registro de Historia Clínica de cada uno de los pacientes que son atendidos en la Institución, al igual que la información administrativa y financiera; por lo tanto y tomando esto como punto de partida se definió realizar un Análisis e identificación de riesgos a los que se encuentra expuesta la Infraestructura de la red de datos de la institución, para de esta manera identificar amenazas que puedan atentar contra la seguridad informática y de los datos de la Institución. Para iniciar el proceso de recolección de información se inició con una entrevista al personal responsable de las redes de datos de la Institución, donde se identificaron algunos aspectos importantes que van en contravía de la seguridad informática; posteriormente se realizó una inspección física a cada una de las sedes que componen la Entidad, con énfasis en la revisión e identificación visual de cada uno de los componentes que hacen parte de la Infraestructura de la red de datos, finalmente se ejecutaron unas pruebas de penetración, haciendo uso de herramientas basadas en Software Libre, sobre la red de datos, cada uno de los hallazgos fueron recopilados y posteriormente plasmados en el documento final; y de acuerdo a estos se planteó una propuesta de mitigación de los mismos como plan de mejora, los cuales se entregaron a la Coordinación del área de Tecnología de la Institución con el fin de ser evaluados y ejecutar las medidas que crean necesarias y se ajusten a la capacidad de la Empresa. En la entrega final del proyecto se puede evidenciar que los objetivos propuestos se cumplieron, y el detalle del desarrollo de la propuesta.
Palabras Claves:	Seguridad, Información, Vulnerabilidad, Riesgo, Auditoria, Activo, Red, Sniffing, Pentesting, Infraestructura, Disponibilidad, Confidencialidad, Integridad.
Contenidos:	Introducción Planteamiento del problema Formulación del problema Justificación Objetivos Objetivo general Objetivos específicos Marco de referencia Antecedentes Marco conceptual Marco contextual Marco Legal

	Diseño metodológico Tipo de investigación Alcance del proyecto Recolección de información Tratamiento de la información Metodología de desarrollo Desarrollo del Proyecto Hallazgos de la Investigación Resultados y Discusión Conclusiones Recomendaciones Divulgación
2. **Descripción del Problema de Investigación**	
Planteamiento del problema:	La ESE Hospital Santa Mónica, al ser una Institución de Salud, maneja información altamente sensible de cada uno de los pacientes que son atendidos en la Entidad, al igual que toda la información que se genera de su accionar asistencial y administrativo; por lo tanto se requiere minimizar el riesgo al que se encuentra expuesto, el Sistema de Información en general de la Entidad, realizando una identificación de debilidades, vulnerabilidades y riesgos, enfocada a la infraestructura de redes de datos, con el fin de dar las recomendaciones, para su posterior mitigación por parte del área encargada en la institución.
Formulación del problema:	¿Cómo minimizar las amenazas y vulnerabilidades presentes en la infraestructura de redes de datos que afectan la seguridad de la información de la E.S.E. Hospital Santa Mónica?
3. Objetivos	
General:	Realizar un análisis e identificación de riesgos, a la infraestructura de redes de datos de la E.S.E. Hospital Santa Mónica de Dosquebradas Risaralda, que sirva como insumo para el aseguramiento de la red de datos de la entidad y seguridad de la información.
Específicos:	• Identificar cada uno de los componentes de tipo Hardware que hacen parte de la infraestructura de la red de datos de la Institución. • Ejecutar un hacking ético, apoyado en las herramientas disponibles de Pentesting, basadas en software libre, con el fin de identificar las vulnerabilidades y riesgos a los que se encuentra expuesta la infraestructura de la de redes de datos de la entidad. • Generar las recomendaciones de acuerdo a los hallazgos detectados sobre la infraestructura de la red de datos, para su posterior mitigación por parte de la entidad, de acuerdo a los resultados obtenidos en las fases previas y al hacking ético. • Diseñar un plan de mejora, de acuerdo al diagnóstico arrojado que impacte directamente cada una de los hallazgos encontrados a la infraestructura de la red de datos de la Entidad.

	• Entregar informe técnico al responsable del área de sistemas de información, que contenga: Los hallazgos, El plan de mejoramiento y las acciones a implementar. Todo lo anterior enfocado a la toma de conciencia por parte de la institución, en beneficio de la preservación de la seguridad de la información.

4. **Metodología**

Después del análisis de diferentes métodos para la implementación de Sistemas de Gestión de Calidad, se pudo evidenciar, que la herramienta más recomendada es la aplicación (Planear – Hacer – Verificar - Actuar), el cual es un ciclo lógico que además de la implementación, permite el fortalecimiento y sostenimiento del sistema de gestión, inmerso siempre en la mejora continua.

Teniendo en cuenta, que el alcance del presente proyecto es de identificar (Debilidades y riesgos), y recomendar (Acciones de mejora); solo se ejecutarán los ciclos de planeación y ejecución, del ciclo PHVA, ya que la verificación y acción le corresponderá a la institución, cuando se implementen las acciones propuestas y realicen el seguimiento correspondiente.

En la etapa de Planeación de plantean las siguientes actividades:

- Obtener la aprobación por parte del área directiva de la organización objeto de estudio, aval que ya se encuentra oficialmente firmado por la Gerencia de la Institución y la Coordinadora del área de Sistemas de Información.
- Definir el alcance del desarrollo del trabajo de grado, el cual se encuentra delimitado dentro del planteamiento de los objetivos y la metodología de la investigación.
- Realizar el inventario de activos correspondientes a la infraestructura de la red de datos de la Institución.
- Levantar la información correspondiente, haciendo uso de las diferentes técnicas de recolección definidas para el desarrollo del proyecto.
- Selección de las herramientas de monitoreo basadas en software libre.

Y finalmente en el Hacer se ejecutan las siguientes actividades

- Identificar las debilidades, riesgos y vulnerabilidades que afectan directamente los componentes que hacen parte de la infraestructura de la red de datos de la Institución.
- Entregar a la Coordinación de Sistemas las recomendaciones y resultados del proyecto.

5. **Conclusiones**

- Se logró evidenciar una serie de vulnerabilidades y debilidades en la Infraestructura de la red de datos, que aunque el personal del área de tecnología tiene identificadas algunas de ellas; las cuales se dilucidaron en la etapa inicial, en la ejecución de la Entrevista, no tenían claro, el impacto o la magnitud del riesgo a el que están expuestos.
- Aunque el área de Tecnología de la información, cuenta con un personal comprometido en cabeza de la Coordinadora, se evidencio gran desconocimiento, en materia de seguridad informática; y que esta no solo pasa con tener configurado un antivirus.

- Se logró demostrar al área de Tecnología de la Empresa que hay una serie de herramientas de Software Libre, disponibles que permiten implementar medidas preventivas a través del monitoreo y detección de vulnerabilidades, sin hacer grandes inversiones económicas.
- Con la entrega al área de Tecnología de la Empresa de las recomendaciones y el plan de mejora propuesto, que salió del presente proyecto, se da un insumo importante para que sea analizado y puesto en marcha en aras de preservar la Seguridad Informática Institucional.
- Las limitaciones que se dan en la Empresa; para la implementación de proyectos de impacto tecnológico, son de orden presupuestal; debido al tipo de Institución, donde en la actualidad el Sector Salud en el país se encuentra en crisis.
- Con la ejecución del proyecto aplicado, se generó conciencia en el personal Técnico del área de Tecnología de la Información, sobre la importancia que tiene mantener en buen estado la Infraestructura de redes de datos; y que esta solamente no se compone de elementos físicos (Switch, Router, Cableado); sino de otros elementos lógicos (Configuración, Políticas), que a la postre son los más importantes bajo la óptica de la Seguridad Informática; ya que son los encargados de minimizar los riesgos e impactos a los cuales se encuentre expuesto la red de datos Institucional.

La Institución ha sido receptiva y colaboradora con la ejecución del proyecto, debido a que son conscientes que el uso de buenas prácticas se traduce en mayor productividad y tranquilidad en cada una de sus áreas, desde la Oficina de Tecnología, hasta la Alta Gerencia.

6. Recomendaciones

- Solicitar a la Gerencia de la Institución la capacitación continua del personal del área de tecnología en temática relacionada con la seguridad informática, con el fin de implementar las mejores prácticas al interior de la institución.
- Implementar las políticas de Seguridad Institucionales, en aras de minimizar los riesgos e impactos a los que se pueda ver abocada la Institución por brechas de seguridad, no identificadas.
- Consultar los manuales de Hardening (Endurecimiento), de cada uno de los dispositivos activos de red, donde se dan las pautas, de las mejores prácticas, para la configuración de los mismos.
- Elaborar el proyecto de actualización de la Infraestructura de la red de datos, sustentado bajo la luz de la seguridad Informática, y apoyado en las diferentes Normas Técnicas que definen los lineamientos para este tipo de Proyectos.
- Revisar, complementar y ejecutar el plan de mejoramiento propuesto, en beneficio de la seguridad Informática Institucional.
- Concientizar a la totalidad del personal de la Empresa, en la importancia del manejo seguro de la información, basado en los lineamientos de la seguridad informática.
- Explorar otros tipos de financiamiento de los proyectos de Tecnología, buscando el apoyo del Gobierno Central; a través de la presentación de estos, al banco de proyectos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Minimizar los riesgos asociados al Sniffing, para evitar este tipo de aplicaciones en la red de la Empresa, se debe partir por implementar controles desde el área de tecnología de la información; iniciando desde los más básicos, hasta los más específicos; para esto se enumeran a continuación algunos a tener en cuenta.

- Limitar y denegar la conexión de equipos de cómputo ajenos a la institución a la red de Corporativa.
- Limitar la ejecución de cualquier tipo de instalador de aplicaciones, en los equipos de la Institución a personal ajeno al área de Tecnología de la Información.
- Explorar e implementar herramientas basadas en Software Libre, para el monitoreo y Detección de Intrusos.
- Realizar un mantenimiento periódico de los equipos de la Empresa a nivel de Software, eliminando todo aquello que no deba estar instalado, en cada uno de los equipos de cómputo.
- Actualizar periódicamente, sistemas operativos y firmware de los Dispositivos Activos de Red (Switch, Router, Servidores, PCs).
- Mantener actualizadas las soluciones de seguridad implementadas al interior de la Institución.

Aquí se dejan algunas recomendaciones que se pueden implementar a nivel general, pero sin dejar de un lado, la actualización permanente de cada uno de los integrantes del área de tecnología en temas relacionados con Seguridad Informática, ya que es una temática con un alto grado de cambio constante.